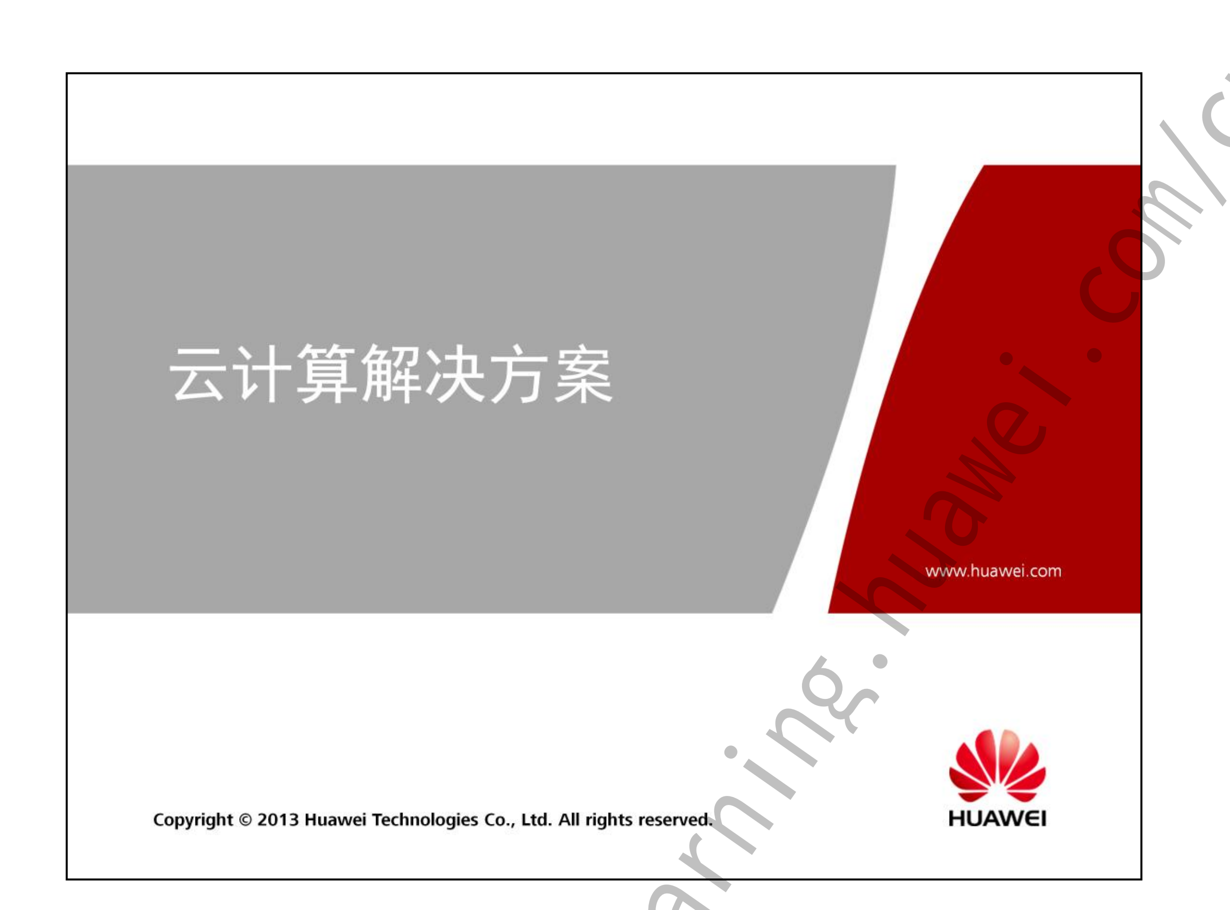
华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- **4、学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform)*，是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。（http://support.huawei.com/ecommunity/bbs/list_2247.html ）




云计算解决方案
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



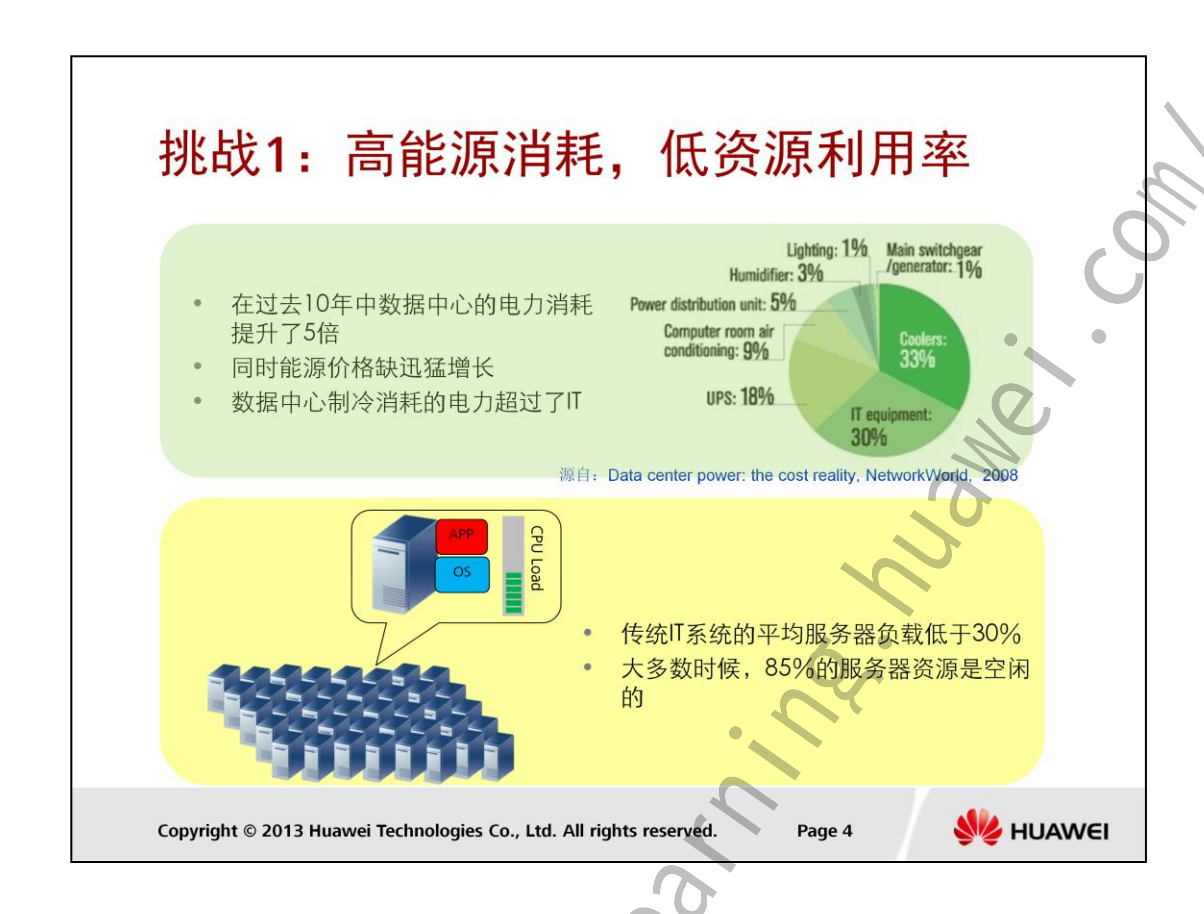
目录





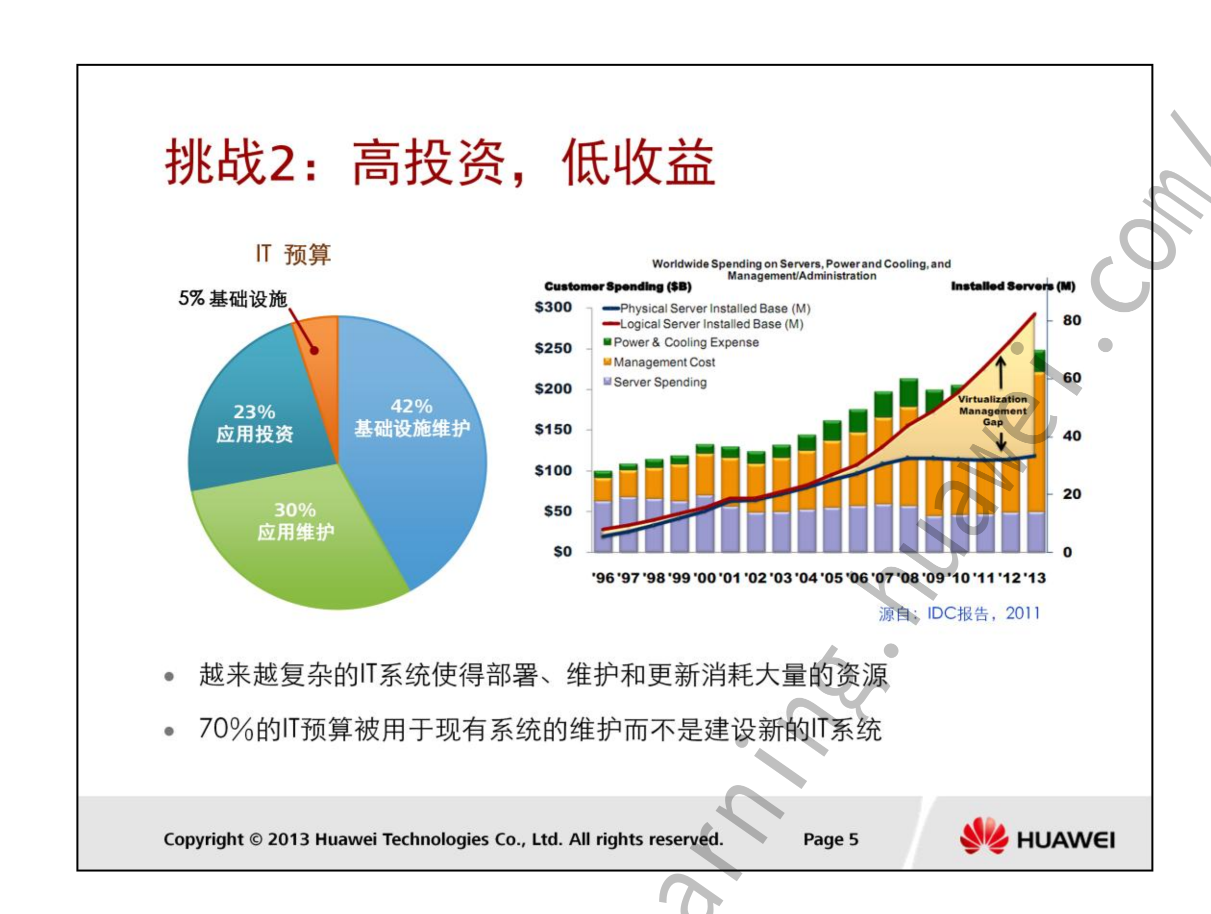
目录





伴随技术和商业的演进，一方面IT系统的市场前所未有的加速成长，但另一方面，传统IT系统却越来越不敷重用，面临巨大的挑战：

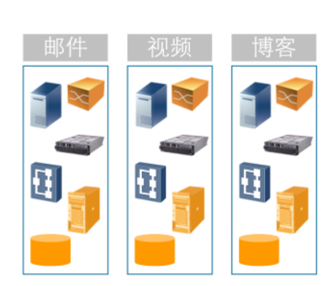
其一是业务所需的计算密度越来越高，从普通机架式服务器到刀片机箱，新的IDC每机柜的能耗从3～5KW猛增至最高20KW以上，这导致能耗居高不下，与此同时，石油价格在过去10年中从不到30USD到现在的100USD，增长了3倍以上。IT系统所支付的电费已经超过购买服务器设备的费用，用于制冷所消耗的电能占整个IT系统能耗的1/3，超过了IT设备的能耗；与此同时，传统IT系统的服务器资源的利用率却很低，相当一部分处于空闲状态的服务器在白白浪费电能。

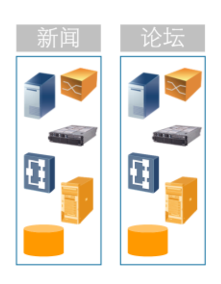


传统IT系统面临的第二个挑战是：

为获得发展优势，投资规模越来越大，但传统IDC的业务模式比较单一，多是各种形式的Hosting出租业务，而这类业务市场竞争激烈，难以获得溢价，属于增量不增收。同时，随着规模扩大，其维护成本显著上升（包括需要的专业技术人员、相应的管理系统等），这是传统IT系统难以解决的问题。

挑战3：迟缓的业务推出速度





- IT系统的部署流程复杂，新业务的上线时间长求
- 烟囱式的IT建设模式，使得不同IT系统间的资源难以共享
- IT容量的规划基于业务峰值，不能动态调整，空闲时存在极大的资源浪费

 Page 6 HUAWEI



与单一业务匹配的是传统IT系统面临的第三个挑战：

业务推出速度缓慢，无法跟上市场节奏。传统的IDC业务，在取得客户需求后，需要经历一系列的步骤：申请预算、购买设备、安装软硬件、系统配置、测试联调、试运行，最后才能投入市场，所需时间一般是1到3个月，甚至更长。

伴随这些不同的业务采购的硬件设备很可能品牌、型号众多，无法统一利用、共享资源，且需按照最大的容量规划预留IT能力，如果业务量动态变化幅度较大，会造成极大的闲置和浪费。



目录





如何面对上述挑战。

来自Gartner的分析表明，全球CIO和CTO们从2008年到2011年，一致认为绿色、虚拟化和云计算位列未来引领IDC发展的十大技术之中。

其中，绿色（高能效、低能耗）越来越收到广泛的关注。在运营商领域：欧洲运营商积极推动节能标准制订并把节能要求写入标书。北美的运营商正在制定设备节能准入标准，并要求第三方认证。中国的运营商已经开始把节能当作一项重要的政治任务。

云计算和虚拟化

- 云计算定义：通过网络将IT能力以大规模、可伸缩、服务的方式进行提供的一种计算模式
- 云计算的价值：高IT资源利用率、高能效、快速服务部署
- 云计算的关键特征：

业务模型 基于使用习惯	按使用付费，像用电一样使用基础设施
习得模型 基于服务	只关注结果，不想了解IT是如何部署
技术模型 动态和灵活性	可以按需扩展和缩减IT容量
访问模型 Internet, Intranet	可以随时随地通过任何设备访问服务

 Page 9



云计算（包括虚拟化），改变了IDC的传统业务模式。

它具备几个核心的特点：按使用付费、高效部署、可动态扩展、随时随地访问。云计算通过分布式的IT设备结合高速网络、虚拟化软件和自动化调度软件，实现了以往在大型主机中才能实现的高可用、无限扩展、简易的集中式管理，而且与大型主机相比，云计算的购置成本和运营成本都低的多；伴随X86芯片处理能力的高速增长，由x86服务器构成的云计算资源处理能力也将快速增长。

简单来说，由于IT 基础架构的有效性和灵活性，云计算使得业务灵活性大大的提高了。



目录



云计算的核心技术优势

技术	◆ 业界领先的虚拟计算、存储、网络技术
管理	◆ 统一云平台部署、管理 ◆ 虚拟机HA，故障快速自恢复，简化维护 ◆ 资源自动调度减少人为干预
用户	◆ 聚焦业务 ◆ 硬件和虚拟机OS 由管理员维护，包括资源分配、故障处理等

优 势

优势1	减少硬件投资	优势2	业务快速上线	优势3	提高资源利用率
优势4	统一维护	优势5	故障自动恢复	优势6	绿色节能

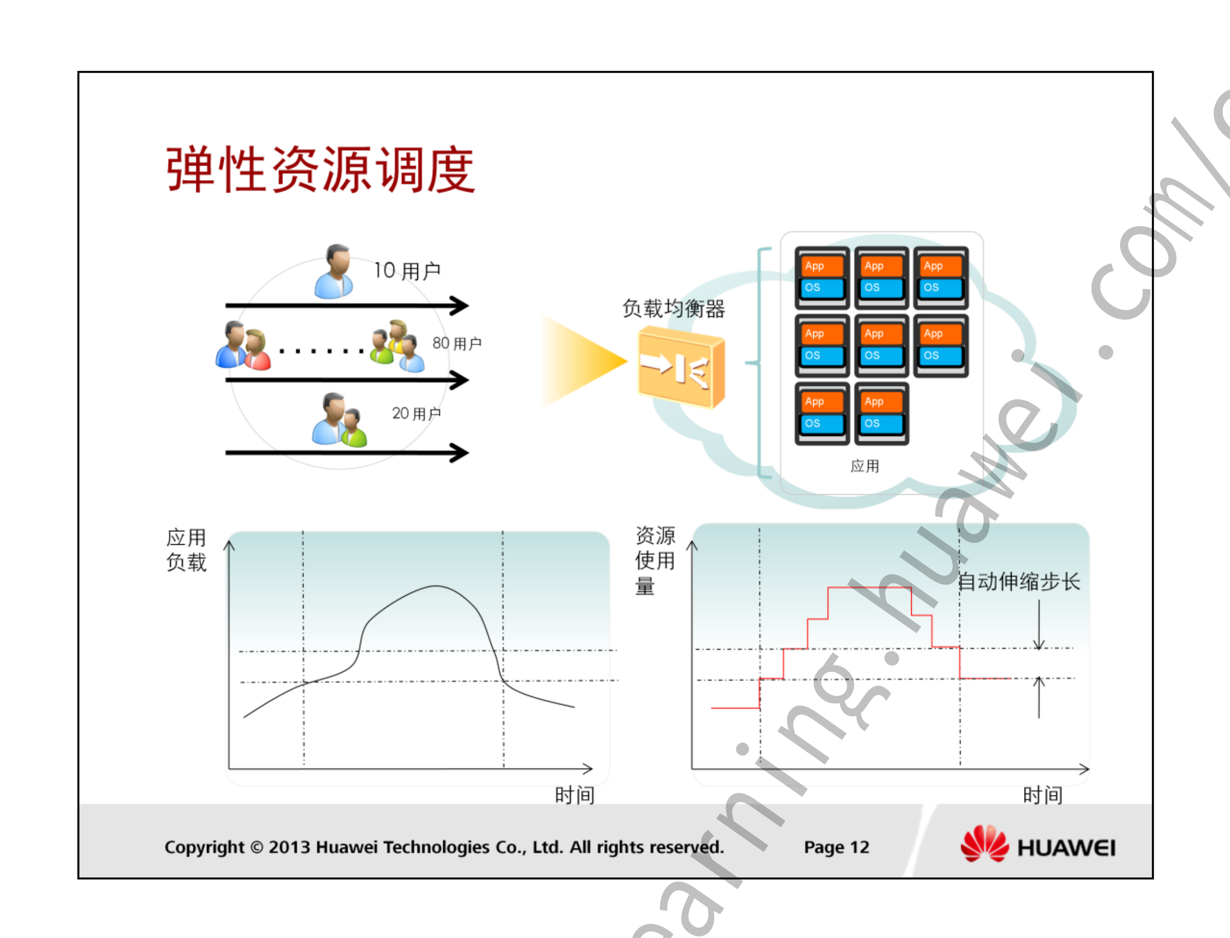
HUAWEI

1技术:

虚拟计算技术，实现资源共享、超分配、灵活分配

虚拟网络技术，实现虚拟和物理网络统一管理，二、三层网络安全

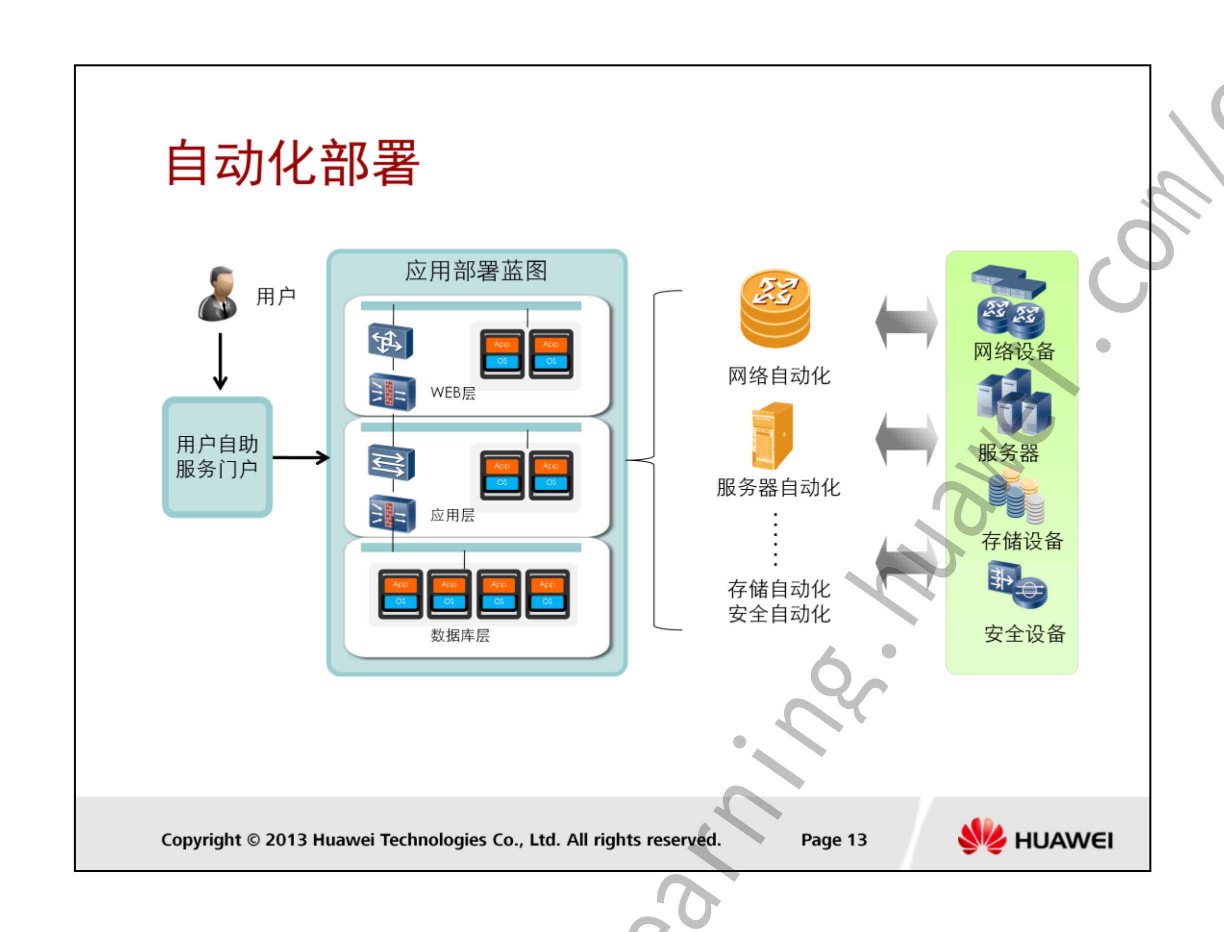
虚拟存储技术，各种物理存储设备统一管理，快照、链接克隆等



与业务匹配的动态资源调度能力，使企业可以灵活的管理自己的IT支出。

比如当前流行的SNS、视听和游戏网站，其用户总体规模虽然庞大，但在一天内、一周内、一月内和一年内的不同时段用户的波动范围很大（50%以上），如果租用IDC的资源，传统模式下要求其IT容量规划必须按照最大规模配备，否则就会降低用户体验。这部分投资不仅巨大，而且多数时候处于闲置浪费。

采用云计算，IT资源可以随需弹性伸缩，而只需为实际使用的资源总量付费，成本可降低75%以上。而且这种模式对IDC运营商和用户是一种双赢。



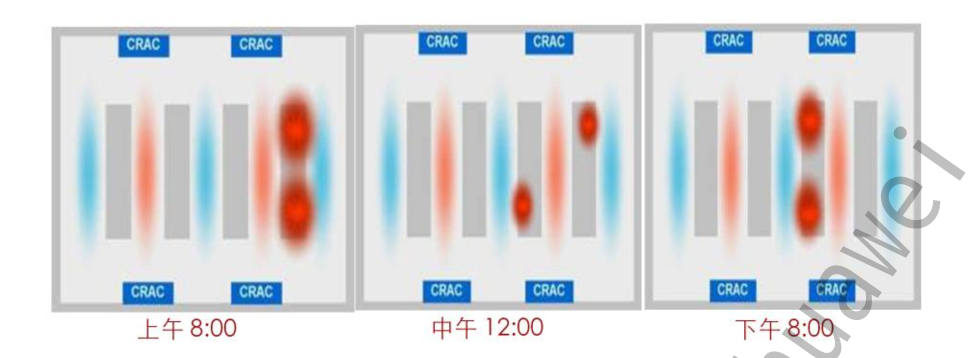
传统的IT业务，如果要上线需经历多个阶段，从硬件部署、软件部署、测试、试运行等，费时长且需要专业IT人员参与。

云计算，自助服务是其最大的亮点之一。无需专业IT人员参与，业务就绪时间缩减至数分钟。

1、对专业的IT人员，可以通过自助服务门户快捷的订购虚拟机、网络服务、安全服务。

2、即使是一个完全不懂IT的业务人员，只要是管理员针对常用的系统做好了架构设计，同样可以通告自助门户获得自己需要的服务，比如一个网站设计人员可能不懂服务器、网络设备和数据库如何配置，但通过模板化的应用部署蓝图，只需几次点击就可以获得一个可立即提供服务的网站框架，而这一切后台的资源配置、软件配置都是自动的、对用户无感知的。

绿色节能



- 动态制冷平衡：自动为热点区域增加制冷量、自动从过热区域迁走虚拟机
- 动态电力平衡：基于IT负载情况自动下电空闲设备

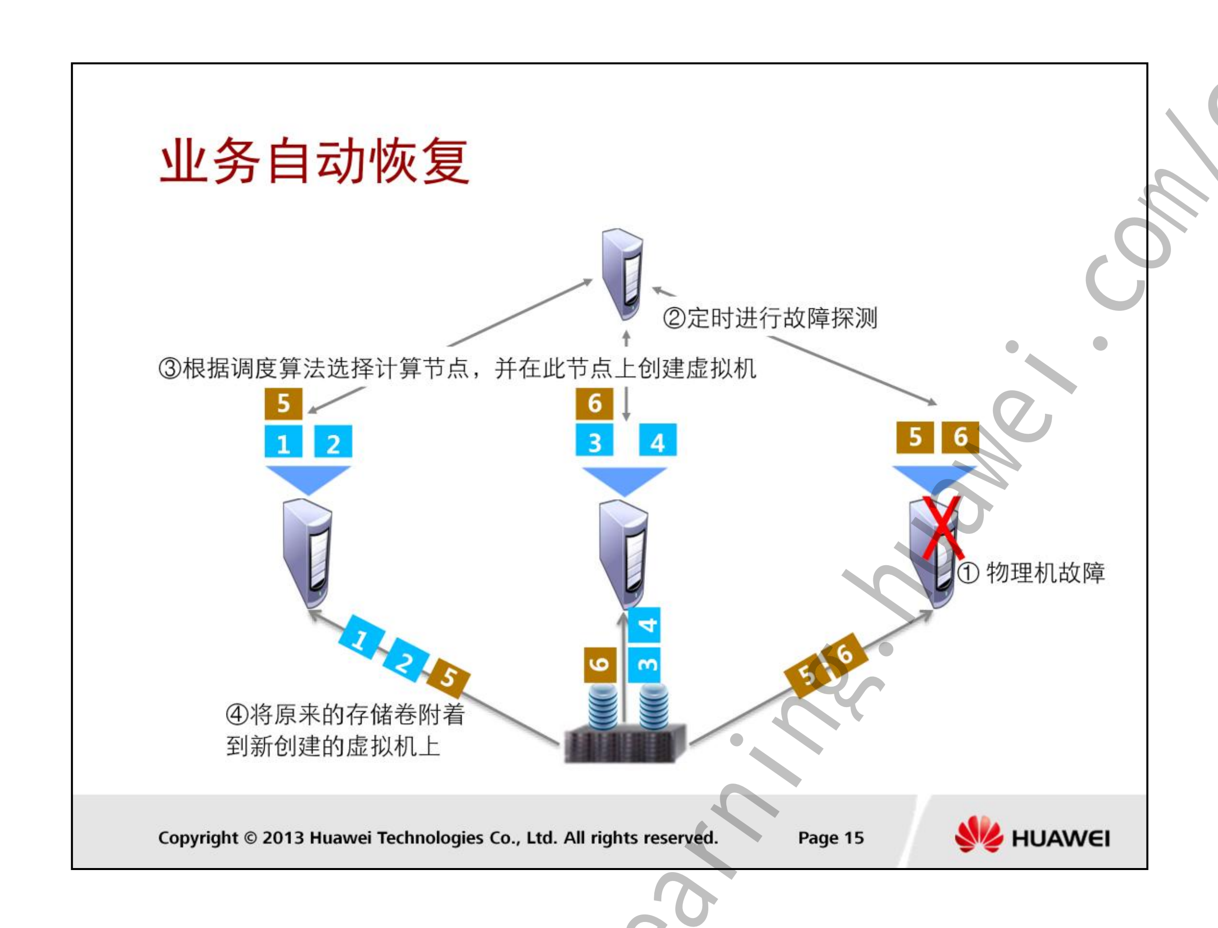
 Page 14



与IT的弹性对应的是机房基础设施的弹性：

1、冷量随IT设备的需要实时调节，适应虚拟化技术和高密度部署，轻松解决热点问题；并且当区域内IT设备的负载量过大导致散热不畅时，自动联动IT管理系统在区域间平衡负载，减少设备故障几率

2、当负载降低、IT设备空闲时，自动联动IT管理系统将虚拟机有效集中，并关闭空闲设备以节电、节冷



应用场景：对于希望长期无人值守自动运行的系统，使用该功能可以有效的避免业务中断

1、物理服务器或虚拟机故障时，系统自动迁移虚拟机到另一可用物理服务器上

2、能检测到的虚拟机OS故障包括：Windows蓝屏，Linux Panic、BUG_ON、Oops等

3、业务中断时长为重启虚拟机的时长

流程：

1、VM故障或计算节点故障。

2、管理节点查询VM状态，发现VM故障

3、管理节点判断VM有HA属性，则根据保存的VM信息（规格、卷），启动新的VM

4、CNA节点收到HA请求，根据VM规格、卷信息创建新的VM。

5、创建过程中，将VM之前的卷重新挂载，包括用户卷。



目录





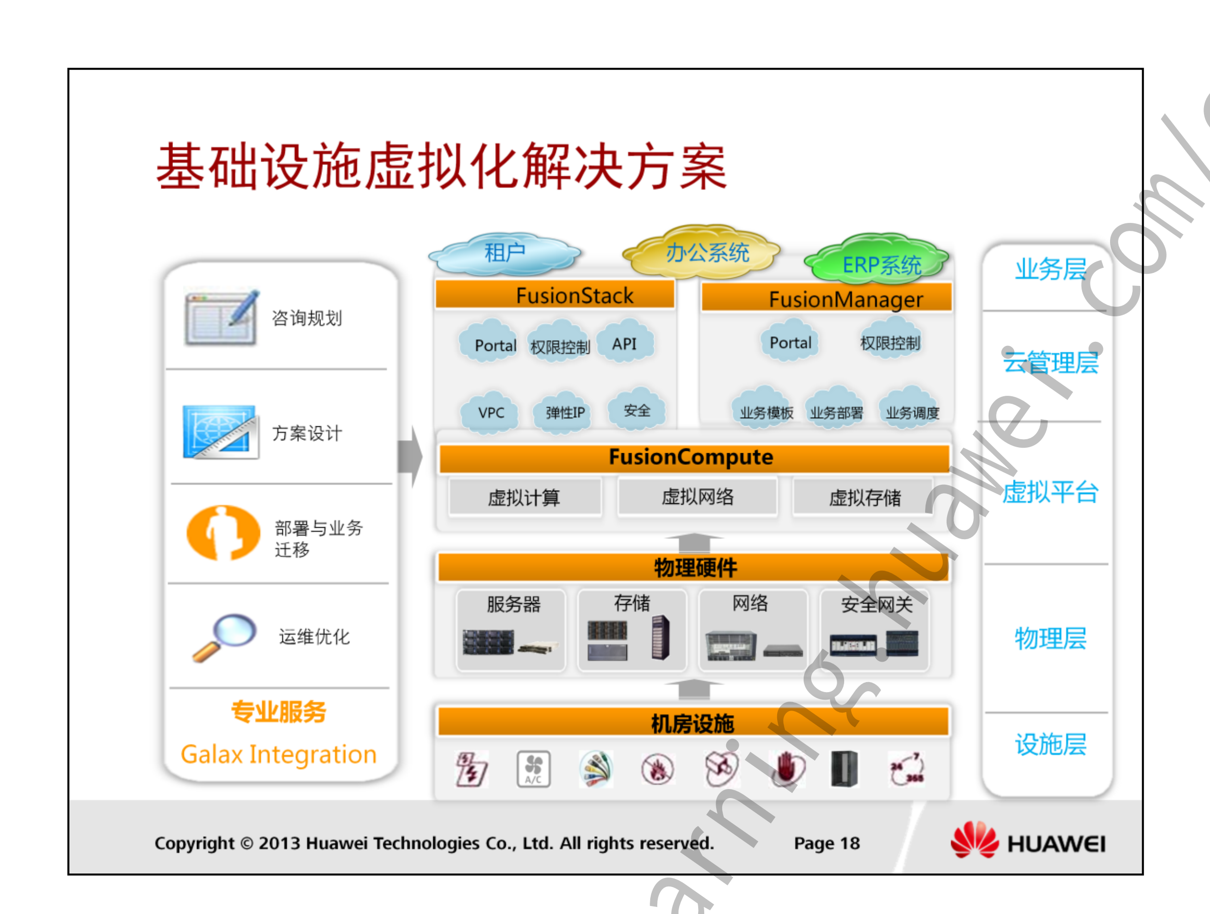
目录

2. 云解决方案概览

2.1 华为云计算解决方案

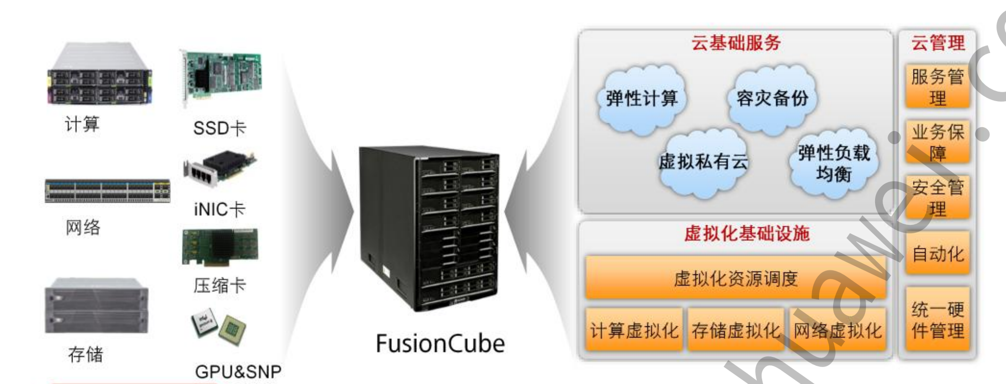
2.2 软件架构





基础设施虚拟化解决方案
咨询规划
方案设计
部署与业务迁移
运维优化
专业服务
Galax Integration
租户
办公系统
ERP系统
FusionStack
Portal
权限控制
API
VPC
弹性IP
安全
FusionManager
Portal
权限控制
业务模板
业务部署
业务调度
FusionCompute
虚拟计算
虚拟网络
虚拟存储
物理硬件
服务器
存储
网络
安全网关
机房设施
业务层
云管理层
虚拟平台
物理层
设施层
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 18
HUAWEI

一体机解决方案 — FusionCube



亮点

- 华为云管理提供一体化管理，自动化部署和高效运维
- 计算，存储，网络垂直整合的融合架构硬件平台OSCA
- 融合存储FusionStorage及SSD应用加速，提升业务敏捷和性能

 Page 19



华为FusionCube一体机的价值

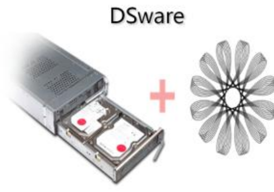
快速部署、高效运维



- 预集成预验证的软硬件融合方案
- 新业务上线从数周缩短至数天
- 统一管理、自动化运维、一键式应用部署，降低OpEx达30%

灵活配比、业务敏捷

DSware



- 全新分布式计算存储融合架构
- 存储性能提升3-5倍
- 支持即插即用的线性平滑扩容，按需扩展

软硬结合、应用优化

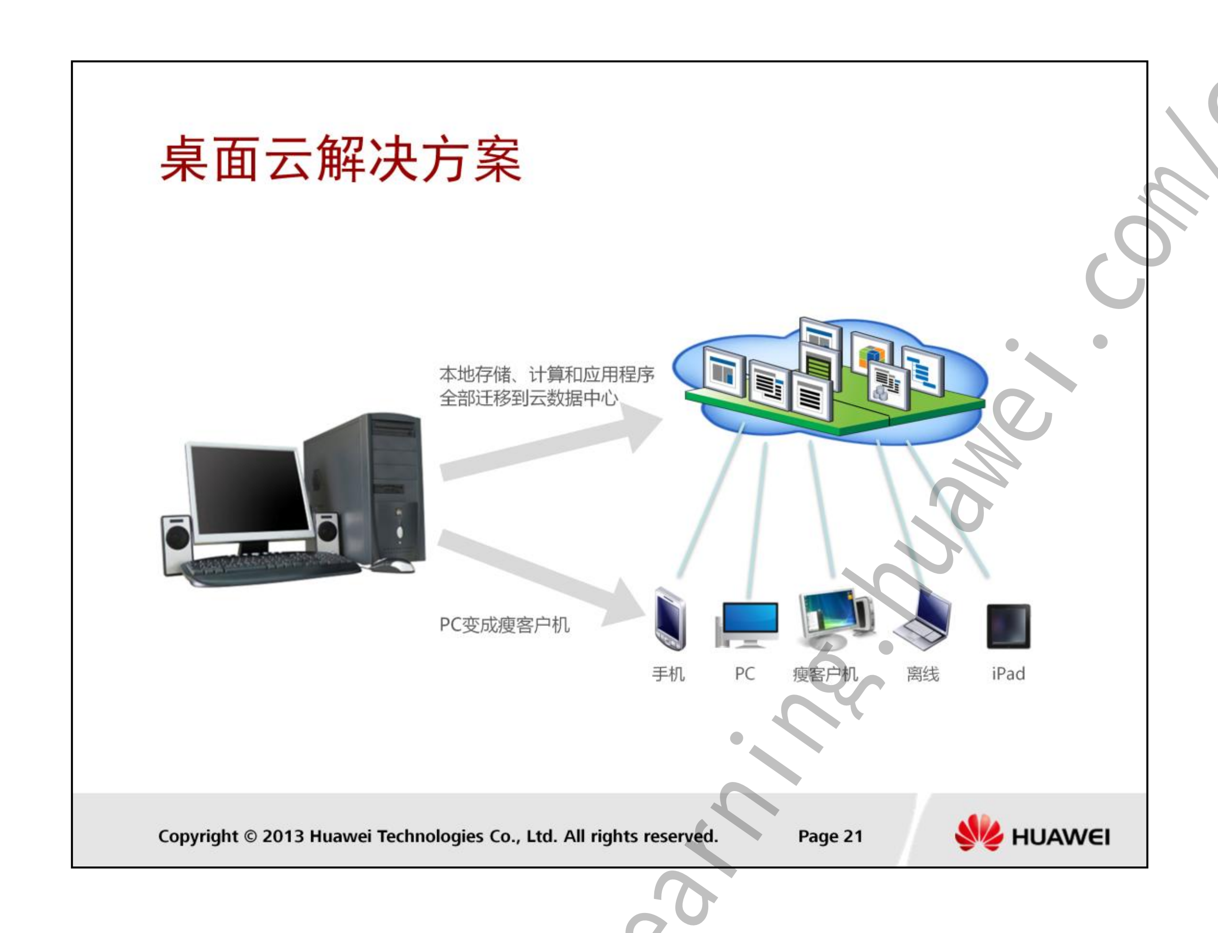


- 高带宽、低时延交换背板
- 多款计算/存储刀片，适用不同场景
- PCIe SSD卡提升IOPS性能1000倍
- 虚拟化智能网卡提升vSwitch性能3倍



企业一站式云平台基础设施

HUAWEI



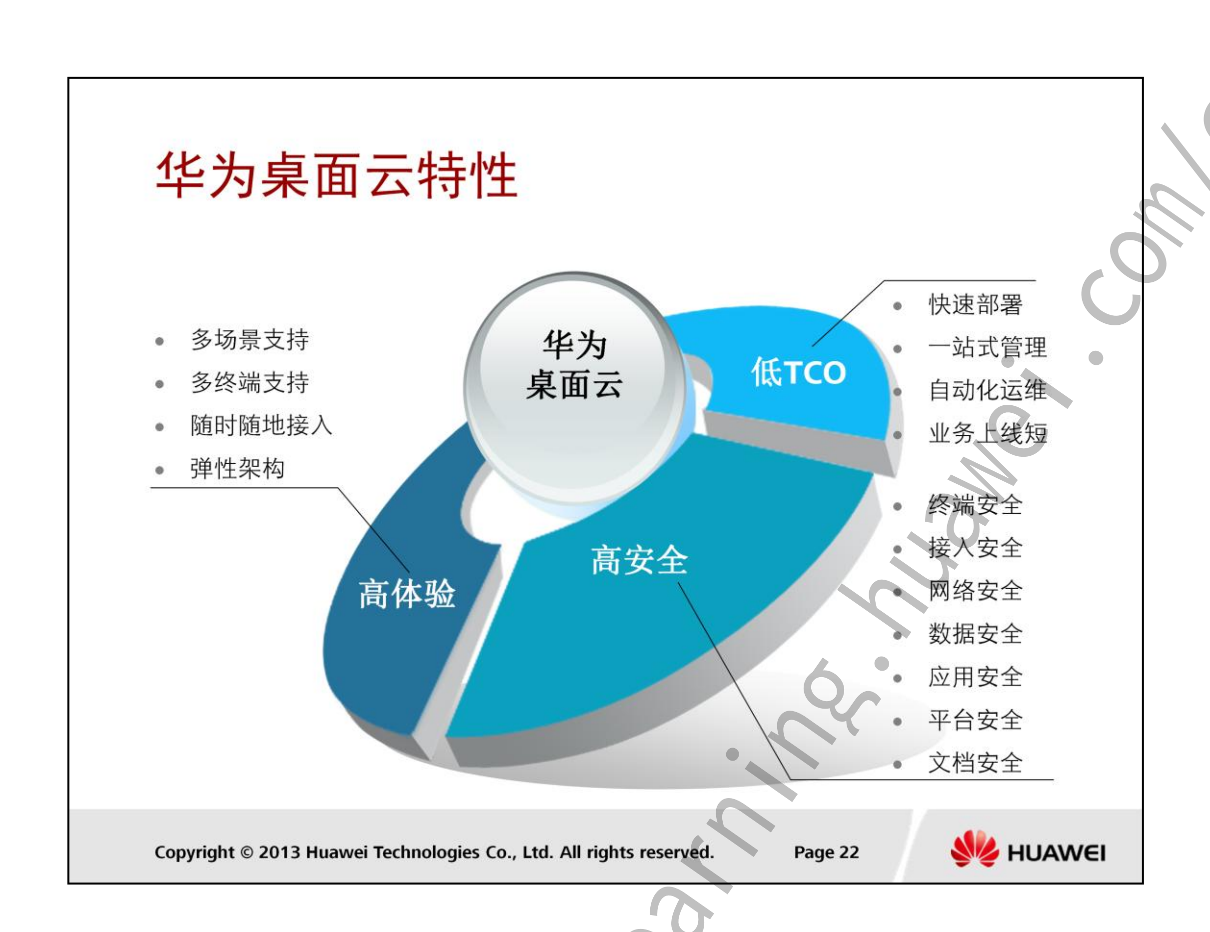
随着革命性技术 – 虚拟化的成熟，办公资源云化已经成为可能。

一个中心：安全 两个基本点：业务体验和综合效率。

1) 利用云计算的技术，将用户的所有应用、数据集中到“云端”，数据中心。

2) 客户通过瘦终端或移动终端访问VM。数据在云端统一存放，将应用和数据以图像方式远程投递，保证数据的绝对安全。

3) 利用虚拟化技术，将云端的计算、存储和网络资源虚拟为虚拟计算机，VM。对使用者而言，这些远端的虚拟VM的使用和一台独立PC相同，能够有自己WINDOWS桌面、自己的应用程序和自己的用户数据。


华为桌面云特性
华为
桌面云
低TCO
高安全
高体验
多场景支持
多终端支持
随时随地接入
弹性架构
快速部署
一站式管理
自动化运维
业务上线短
终端安全
接入安全
网络安全
数据安全
应用安全
平台安全
文档安全
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 22
HUAWEI



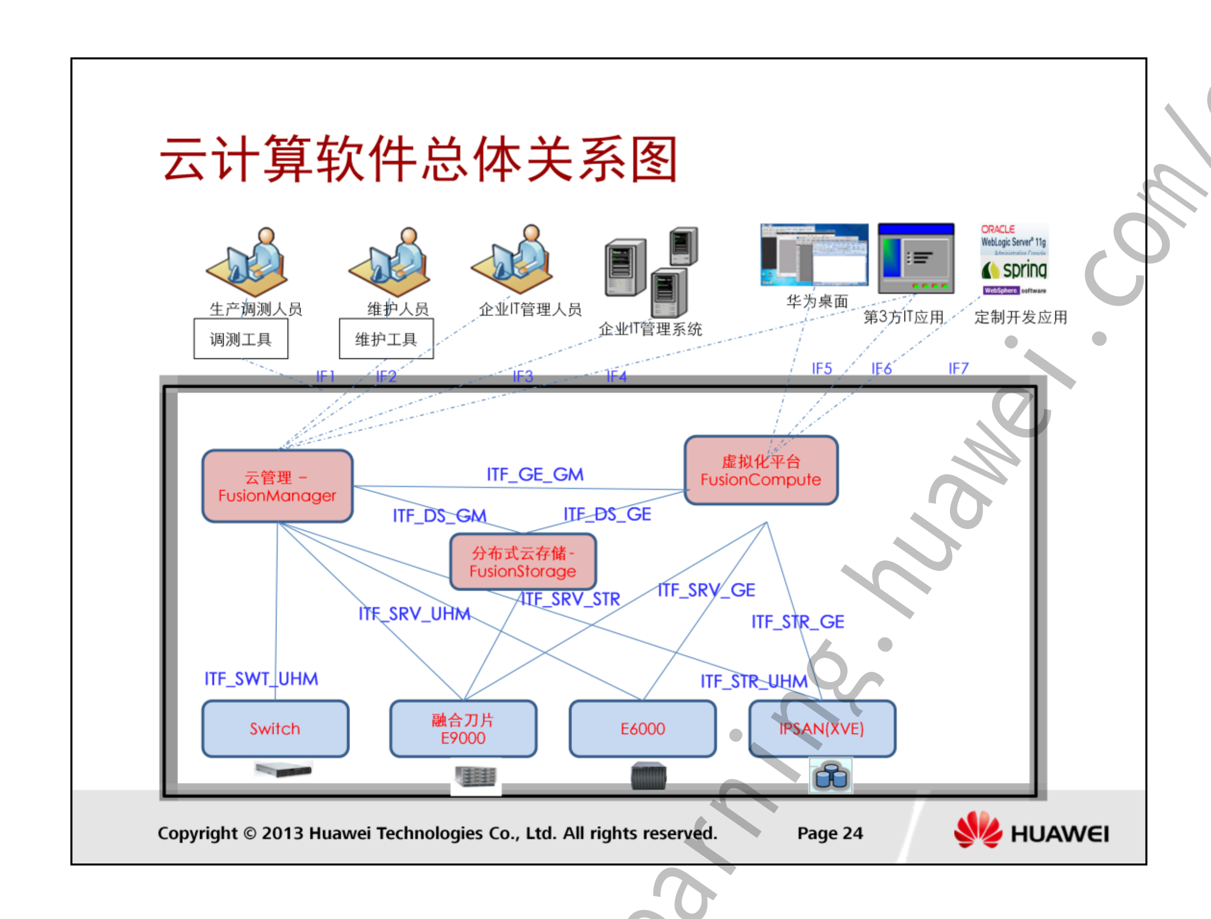
目录

2. 云解决方案概览

   2.1 华为云计算解决方案

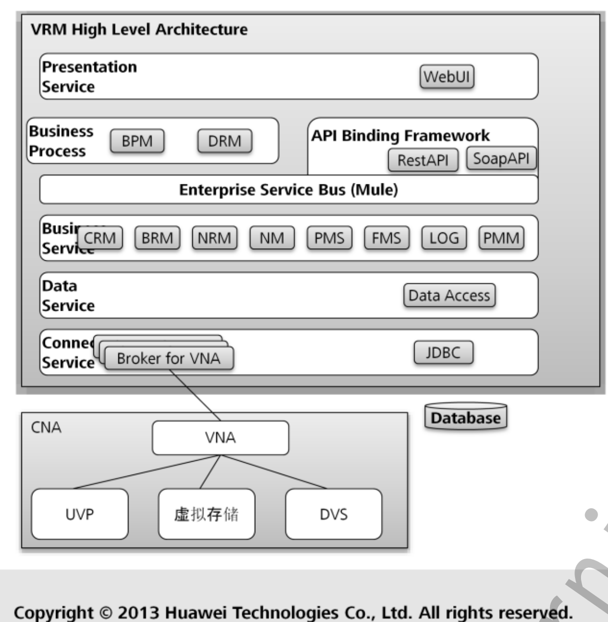
   2.2 软件架构





- FusionCompute：提供基础设施虚拟化功能。以计算虚拟化、存储虚拟化和网络虚拟化为核心，将硬件资源汇聚为资源池并在资源池内提供各种资源调度与服务保障能力。为用户提供高效、可靠、灵活的基础设施虚拟化解决方案。
- FusionManager：提供云管理功能。在支持异构资源池统一管理的基础之上，实现基础设施的云化。对外提供统一基础设施资源发放、跨集群资源调度、应用发放与应用伸缩等能力。包含原来的统一硬件管理子系统，提供对硬件设备的统一发现、自动配置、故障监控能力。
- FusionStorage：提供高性能分布式存储功能。通过将服务器磁盘资源池化和数据的多节点冗余存储实现IO访问的高并发。 对外提供高可靠、高性能、低成本的内置存储解决方案。实现计算和存储的垂直整合

FusionCompute软件架构



- 虚拟基础设施系统由虚拟化管理（VRM）和虚拟化代理（VNA）两部分组成
- 一个VRM对应一个站点，每个站点内包含独立的服务器、存储和网络
- VRM可以将服务器进行逻辑分组，组成集群使虚拟机在集群范围内进行HA调度

 Page 25 

- 表示层：基于Extjs框架实现的前端GUI界面，支持IE8+、Firefox8+浏览器
- 接口层：系统配置、计算、网络、存储、账户管理、监控、告警、补丁管理等功能，基于Rest风格的接口，全能力开放
- 业务逻辑层：对原子能力（计算、存储、网络等）进行编排和组合，按业务需要构造业务流
- 业务能力层：提供计算（cpu、内存等）、网络（vlan、物理网卡等）、存储（卷、raid组等）资源管理能力，以原子接口形式开放
- 数据访问层：使用Hibernate框架将关系型数据封装成数据对象

FusionCompute模块介绍（1/2）

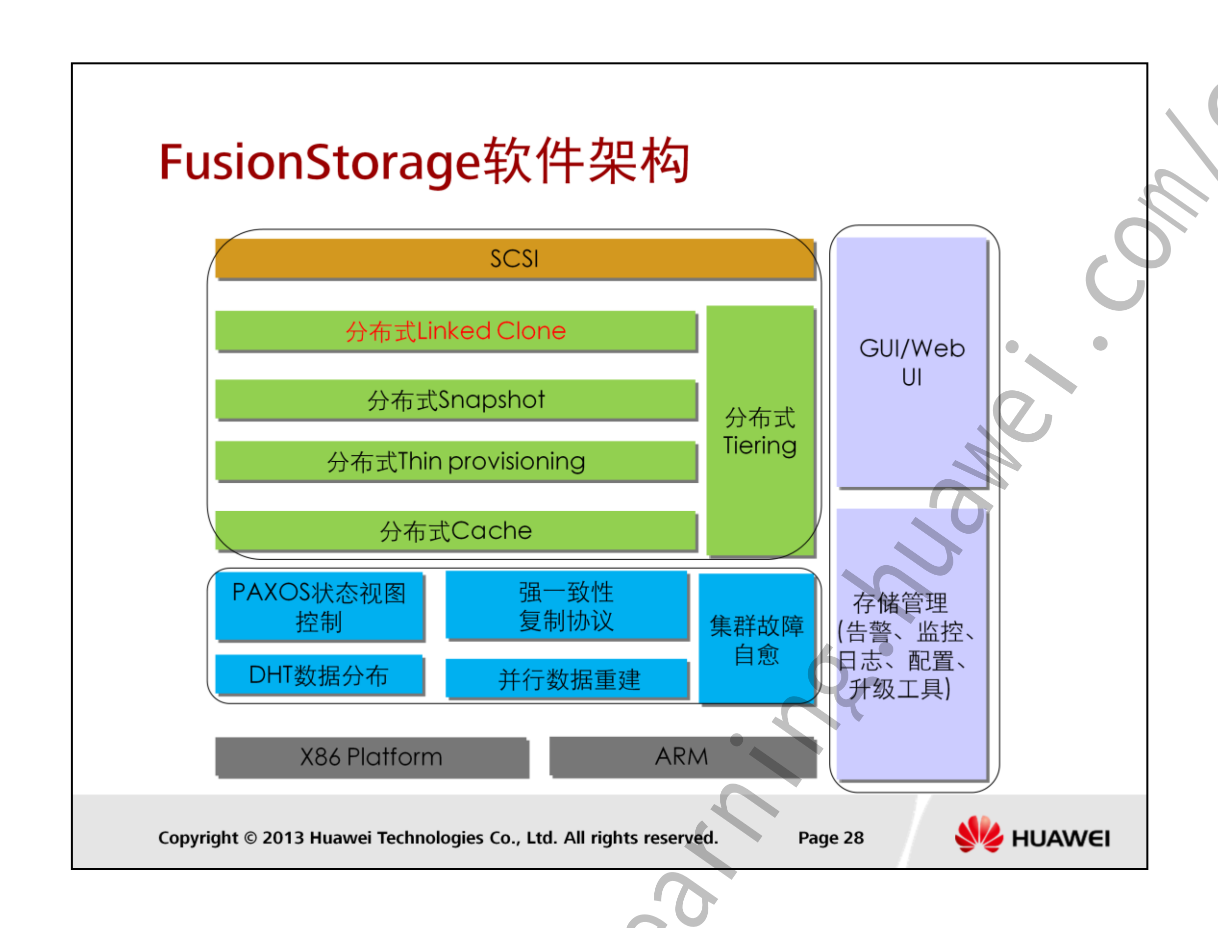
FM名称	功能说明
BPM	负责复杂的资源管理过程，如虚拟机创建的处理
DRM	负责根据一定的策略（节能，负载均衡）进行分布式的资源管理
CRM	负责对虚拟计算资源进行管理
BRM	负责IPSAN、本地存储等存储资源的管理
NRM	负责网络资源的管理
NM	负责对虚拟化节点的管理
PMS	性能管理，负责收集性能数据，进行性能的实时分析和后分析
FMS	故障管理，负责收集告警和故障信息
PMM	补丁管理模块，负责计算节点的补丁管理
LOG	系统的日志功能，用于系统故障的定位。



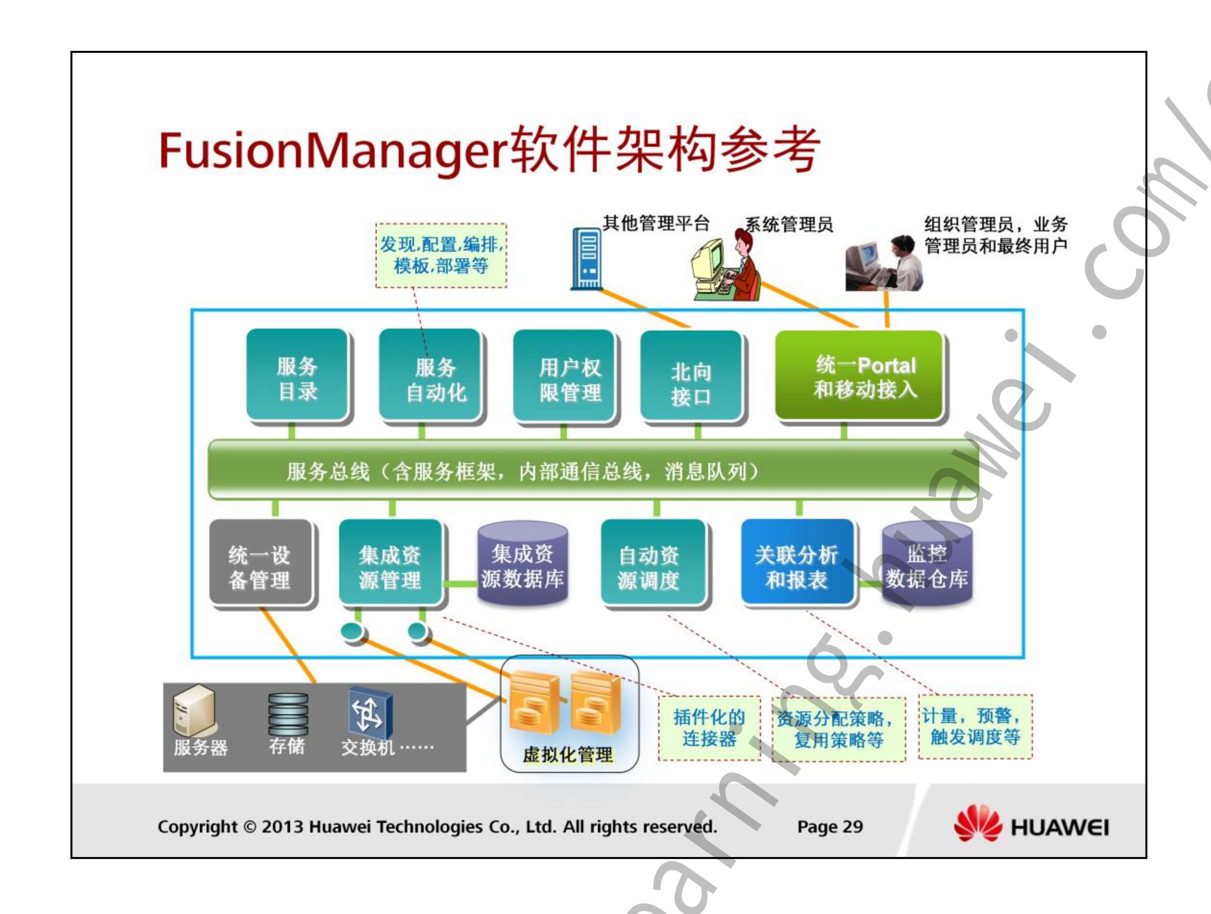
FusionCompute模块介绍（2/2）

FM名称	功能说明
VNA	负责对虚拟化节点上的计算、存储、网络资源进行控制
UVP	统一虚拟化平台，提供计算虚拟化能力
DVS	分布式虚拟交换机
虚拟存储	虚拟存储的功能实体
WebUI	系统的管理Portal，通过API对系统进行管理





- 分布式存储集群控制
  - 分布式存储集群控制，主要实现了强一致性的复制协议，通过PAXOS算法来进行集群节点状态视图的控制，实现了DHT相关的数据分布算法，实现了并行数据重建机制，达到集群硬盘或节点故障自愈的目的。
- 块存储业务
  - 块存储业务所必须的一些基础功能特性和增值功能特性逻辑：分布式读写cache、分布式快照、分布式连接克隆、系统天然支持的分布式瘦分配、分布式Tiering。
  - 对上层应用提供SCSI访问接口与虚拟机Hypervisor集成，对虚拟机提供块设备接口。
- 存储管理
  - 对分布式块存储集群进行告警、监控、日志的管理，同时能够实现对集群的自动化配置、安装部署、在线升级功能。对用户提供Web UI的界面。



- 方框内是FusionManager云管理平台的功能模块。“虚拟化管理”可以采用华为的虚拟化管理软件FusionCompute，也可以采用其他厂家的，如VMware的VCenter+Vsphere等。
- 云管理软件从软件层面拉通统一各资源管理。

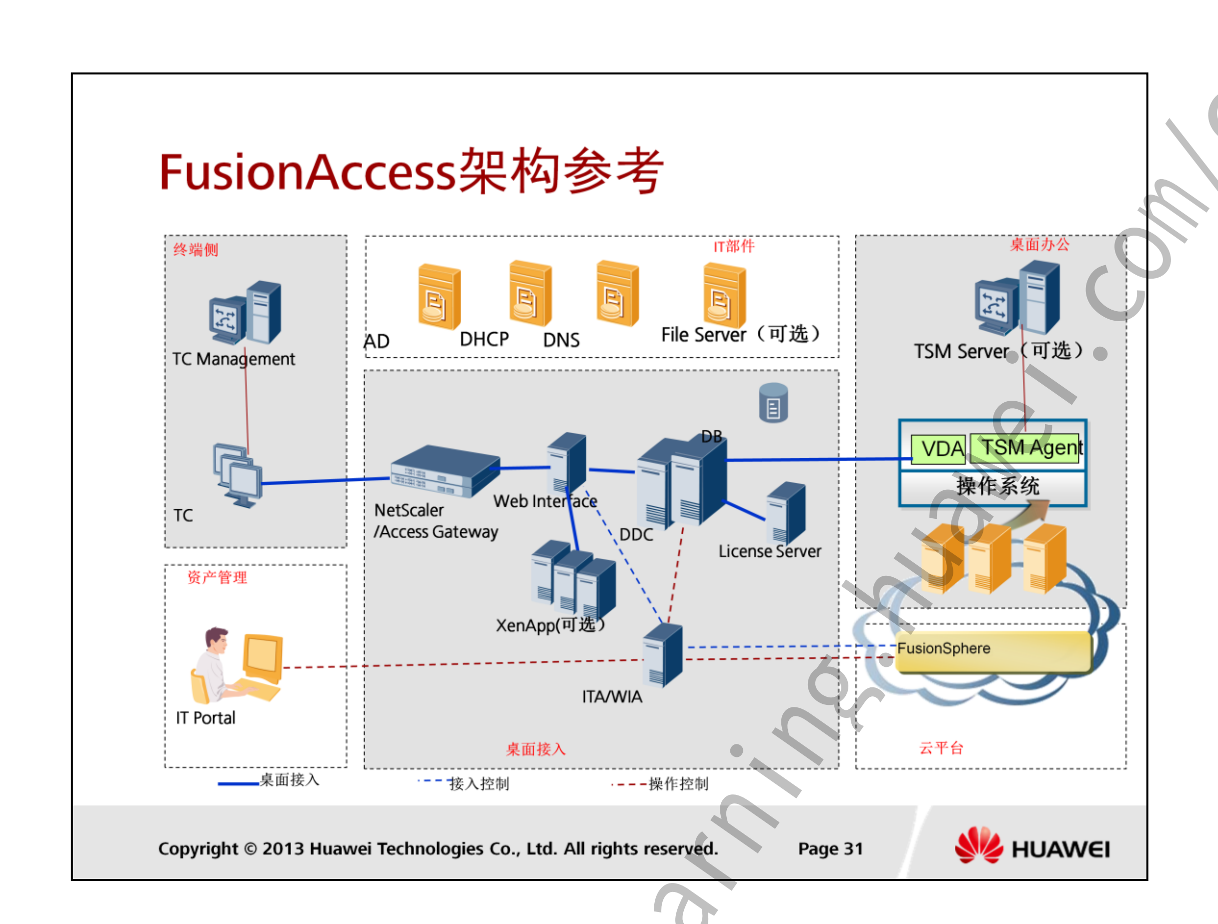
华为云管理模块功能介绍

模块	功能说明
集成资源管理	物理资源管理，虚拟化资源管理，资源集群管理，组织vDC管理
服务目录	服务模板管理，服务目录管理，服务请求，服务实例
服务自动化	服务自动化部署，软件包管理，自动伸缩，服务模板设计
权限管理	包括用户管理、角色管理、角色授权、登陆认证、鉴权等功能，实现全系统的安全功能。同时对外提供LDAP和AD的认证服务
统计报表	性能报表，容量管理
告警	告警集中监控，告警过滤查询，告警转邮件，告警阈值
北向	Restful北向接口，提供告警，性能统计和业务管理功能
UPortal	全系统UI界面的唯一入口

 Page 30



- 组织VDC：组织虚拟数据中心 (orgVDC) 为组织提供资源管理的单元。orgVDC 提供了一个可以存储、部署和操作虚拟系统的环境。orgVDC由系统管理员创建，会指定唯一归属的资源集群，指定计算（CPU和内存）资源配额，指定一个或多个存储DataStore的配额，含vAPP，组织网络。一个组织可以有多个 orgVDC，不 同orgVDC可以通过共享组织网络（orgNet）实现互通。


FusionAccess架构参考
终端侧
TC Management
TC
IT部件
AD
DHCP
DNS
File Server（可选）
桌面办公
TSM Server（可选）
VDA
TSM Agent
操作系统
NetScaler
/Access Gateway
Web Interface
DB
DDC
License Server
XenApp(可选）
资产管理
IT Portal
ITA/WIA
FusionSphere
桌面接入
云平台
桌面接入
接入控制
操作控制
Page 31
HUAWEI

FusionAccess部件

- **终端部件**
  - 硬件：TC
  - 软件：TC Management
- **桌面接入部件**
  - 软件：DDC、License Server、Web Interface、VDA
  - 硬件：Netscaler（含Access Gateway软件）
- **桌面应用虚拟化部件**
  - 软件：XenApp
- **自动化管理部件**
  - 软件：ITA、WIA
- **桌面软件管理部件**
  - 软件：TSM（含Server及Agent）
- **IT架构部件**
  - 软件：AD、DHCP、DNS、File Server





目录



华为为什么部署桌面云



据统计，华为每年
- 有2亿次库存交易
- 70万个客户请求
- 内部每个月有1.6亿封邮件
- 1.7亿条办公信息即时沟通信息
- 60万人次外网访问登录
- 170万人次访问网页
- ……

如此大的数据量存在本地PC？

信息安全？
高效运维？



庞大的IT开销
- 多达数亿的IT运维开销
- 近600万元的电费开销
- 五年多达近6千万的PC购买成本
- ……

降低开销？

员工办公
- 多业务快速部署
- 移动办公
- 多终端办公
- ……

灵活办公？

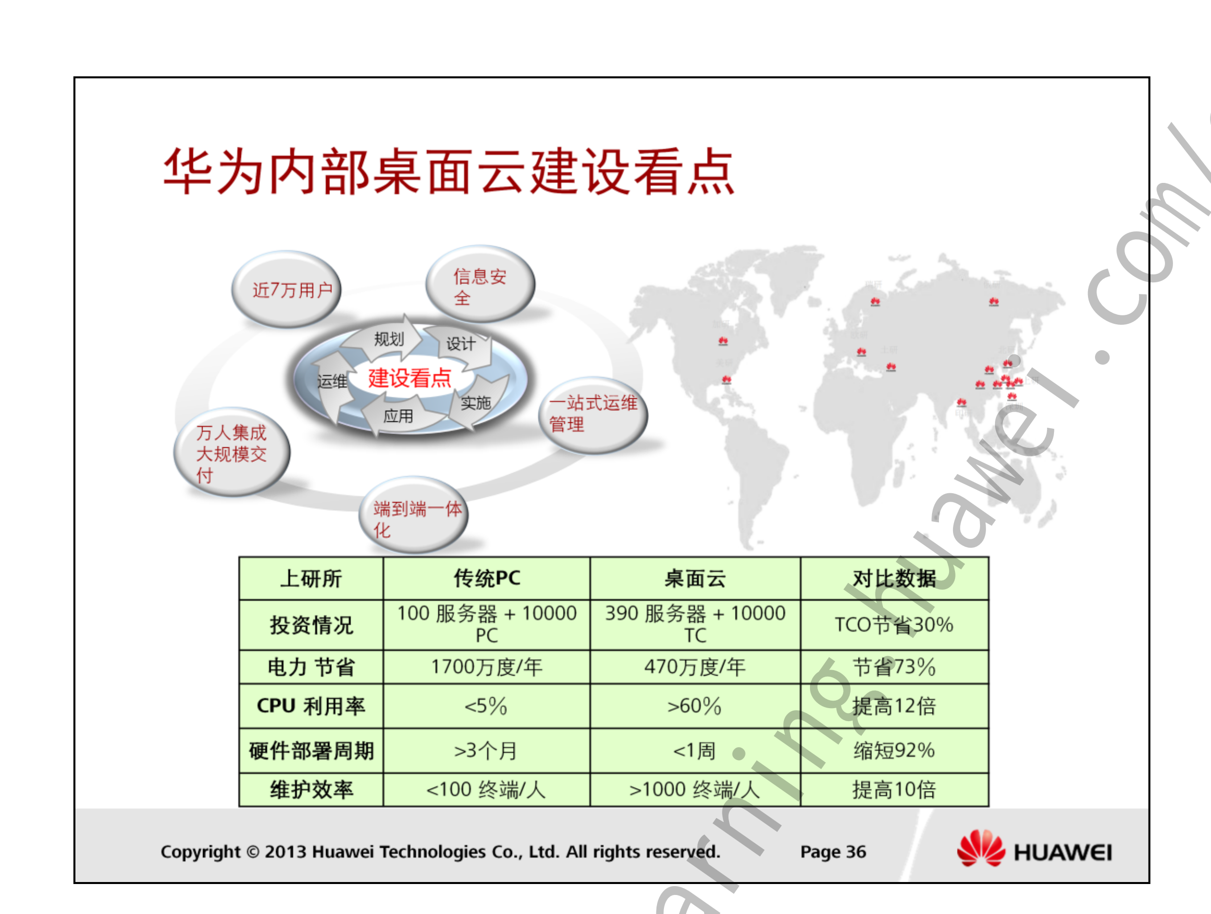




华为公司内部桌面云解决方案全景图

 Page 35 HUAWEI

- 华为公司桌面云的建设历程，强调桌面云的发展是从小到大，从上研的300用户试用到后面的1万桌面云大规格部署，到2011年全公司的铺开建设，目前工程建设总量接近12万，实际上线用户在7万左右（剩下的正在推行，逐步上线）。
- 红区、黄区、绿区隔离，实现数据与信息安全。



上研所	传统PC	桌面云	对比数据
投资情况	100 服务器 + 10000 PC	390 服务器 + 10000 TC	TCO节省30%
电力 节省	1700万度/年	470万度/年	节省73%
CPU 利用率	<5%	>60%	提高12倍
硬件部署周期	>3个月	<1周	缩短92%
维护效率	<100 终端/人	>1000 终端/人	提高10倍



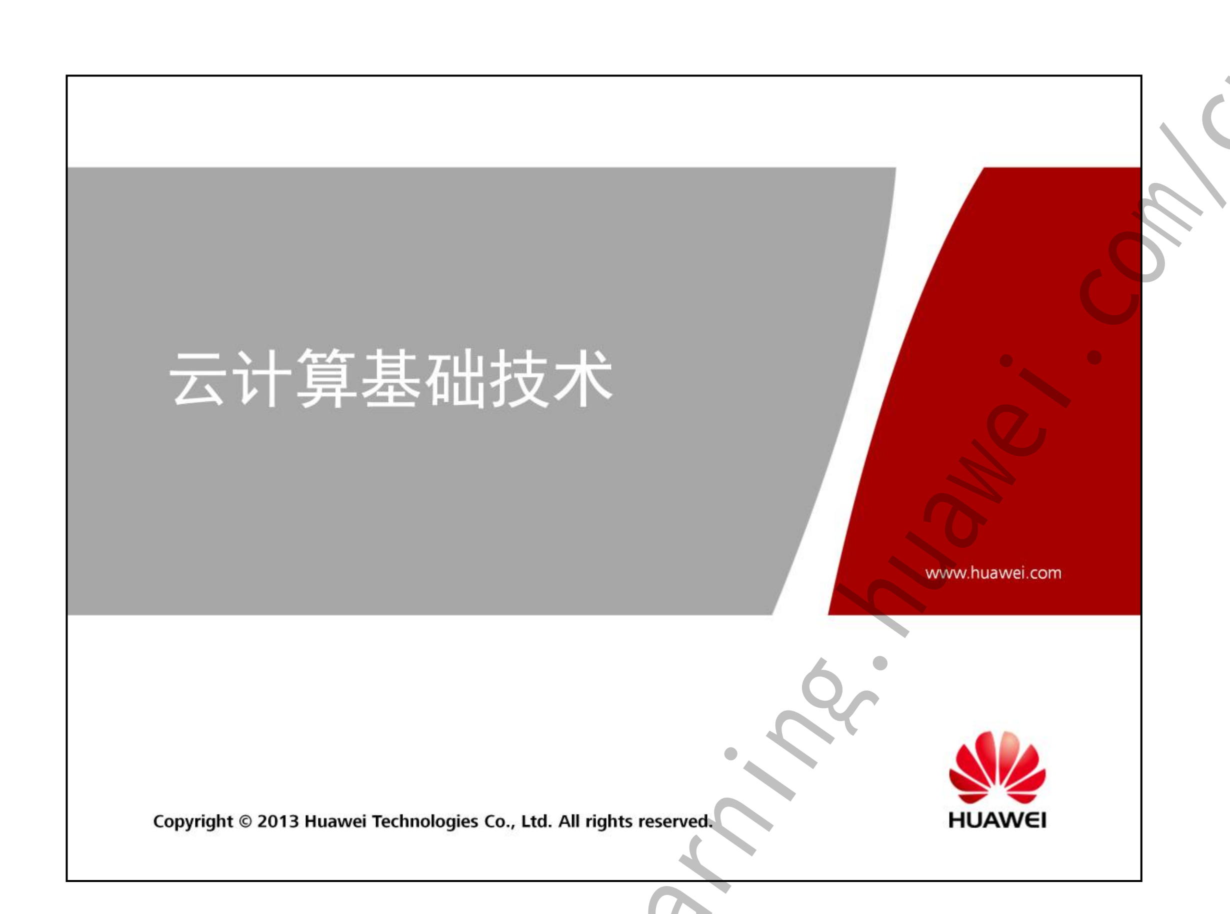
总结

- IT系统的演进
- 云解决方案概览
- 应用案例



Thank you

www.huawei.com


云计算基础技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解云计算领域有哪些基础技术
  - 了解链接克隆技术
  - 了解内存复用技术
  - 了解备份和恢复技术
  - 了解虚拟机快照技术
  - 了解虚拟机迁移技术
  - 了解虚拟机资源在线调整技术
  - 了解动态资源调度技术





目录





- 本页罗列了云技术基础技术的列表，讲解此页时，可以先提问，让学员列举所知道的技术。然后和学员一起浏览一下本页列举的技术
- 链接克隆：链接克隆是指多个虚拟机共享同一份系统卷的技术；用户的数据写入到一个额外的差分卷中（diff disk），而数据读取则从共享系统卷和差分卷中读取。利用链接克隆技术，可以从基础镜像中快速克隆和部署多个桌面，提升桌面分发速率及存储资源占用，适合于桌面高度标准化场景，如营业厅等。同时可通过Intellicache，将共享的系统卷缓存在服务器内存中，提升读取性能
- 内存复用：采用智能内存复用，使服务器上虚拟机的内存总量大于服务器上的物理内存，同样的物理内存条件下能运行更多的虚拟机，延长物理服务器升级内存的周期。复用技术包括内存气泡、内存交换等
- 备份恢复：提供基于虚拟机操作系统内文件粒度备份、存储系统粒度、虚拟机粒度等多种技术的备份和恢复方案
- 虚拟机迁移：虚拟机热迁移是指在不中断业务的情况下，将虚拟机从一台物理服务器移动到另一台物理服务器
- 虚拟机快照：支持把某一时刻虚拟机的状态（所有的硬盘信息、内存信息和CPU信息）像照片一样保存下来，用于虚拟机Guest OS故障等场景的恢复。快照采用增量快照及快照合并技术，使用的存储空间较小
- 虚拟机资源在线调整：支持虚拟机的vCPU、内存、网卡、磁盘等资源在线调整，方便用户根据业务需求调整虚拟机规格
- 资源动态调度：1、采用智能调度算法，根据系统的负载情况，对资源进行智能调度，达到系统的负载均衡，保证良好的用户体验

2、持续监控系统的资源利用率，根据业务需求智能的调整资源：在满足业务性能需求的前提下，根据业务工作负载情况整合物理服务器，使服务器数量最少；同时关闭不需要的



目录

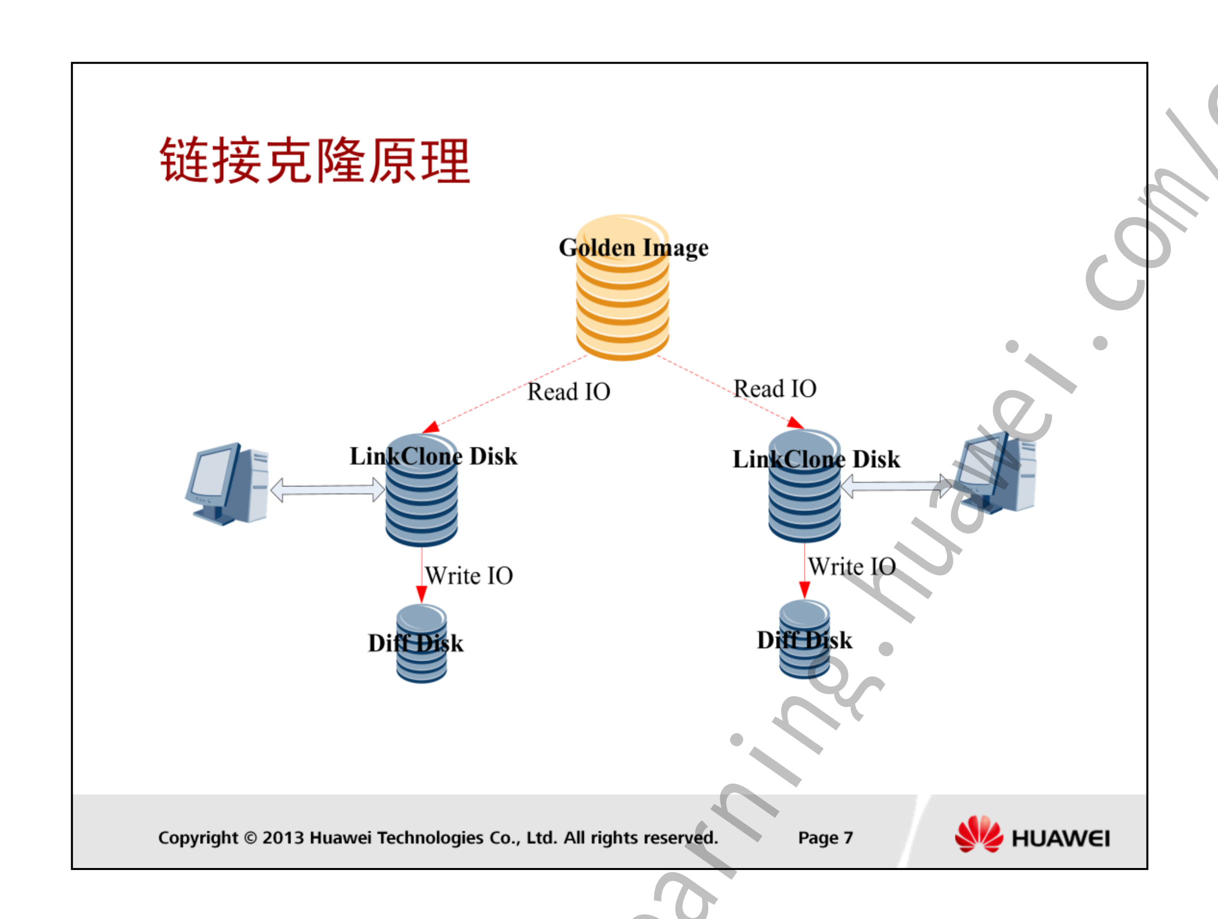


什么是链接克隆？

- 链接克隆是指将母盘和差分盘组合映射为一个链接克隆盘，并将该链接克隆卷提供给虚拟机使用的技术
- 多台虚拟机共享链接克隆卷的母盘（系统盘），但对于链接克隆虚拟机的修改不会影响母盘
- 链接克隆虚拟机具有创建速度快、软件更新快捷、存储资源占用少的优点



- 链接克隆：通俗地讲，就是通过链接的方式克隆一个操作系统的系统盘。从外界来看，初始状态完全是被克隆操作系统系统盘的拷贝，但底层实际上完全链接到被克隆的系统盘，并不占用真正的存储空间。



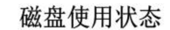
原理

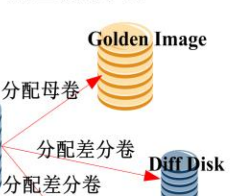
- 在链接克隆的场景下，母盘是只读的，母盘只会提供一个原始的操作系统盘（Golden Image）。在运行过程中，每个操作系统产生的差异化数据都会被保存到差异盘（Diff 盘）中。
- 虚拟机的写流程：虚拟机产生一个写请求，直接写到差异盘（Diff 盘）中。
- 虚拟机的读流程：虚拟机产生一个读请求，首先判断该数据是在母盘中还是在差异盘中，如果是在母盘中，直接从母盘读取；如果是在差异化盘中，直接从差异盘中读取。
- 当前的规格是一个母盘支持128个链接克隆盘。

链接克隆磁盘状态

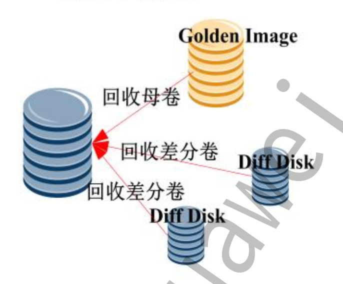
存储初始状态











- 创建链接克隆虚拟机时，如果没有母卷，则先通过模板创一个母卷，然后创建差分卷
- 删除某链接克隆虚拟机时，如果母卷还在支持其他链接克隆虚拟机，则只删除差分卷；如果该母卷下已无链接克隆虚拟机，则删除母卷和差分卷



链接克隆 vs 完整拷贝

	连接克隆	完整拷贝
系统盘存储	• 多个虚拟机可共享一个母卷	• 每个虚拟机，都有独立的母卷
数据存储	• 系统差异数据，保存在差分盘中 • 用户数据，可以保存到各自的数据盘中	• 系统差异数据，保存在各自独立的母卷中 • 用户数据，保存到各自的数据盘中
系统盘还原	• 系统可还原，可以设置还原策略	• 系统无还原功能
虚拟桌面分配	• 动态池：M:N分配方式 • 静态池：1:1分配方式 • 静态池（PvD）：1:1分配方式	• 1:1分配方式或1:N分配方式

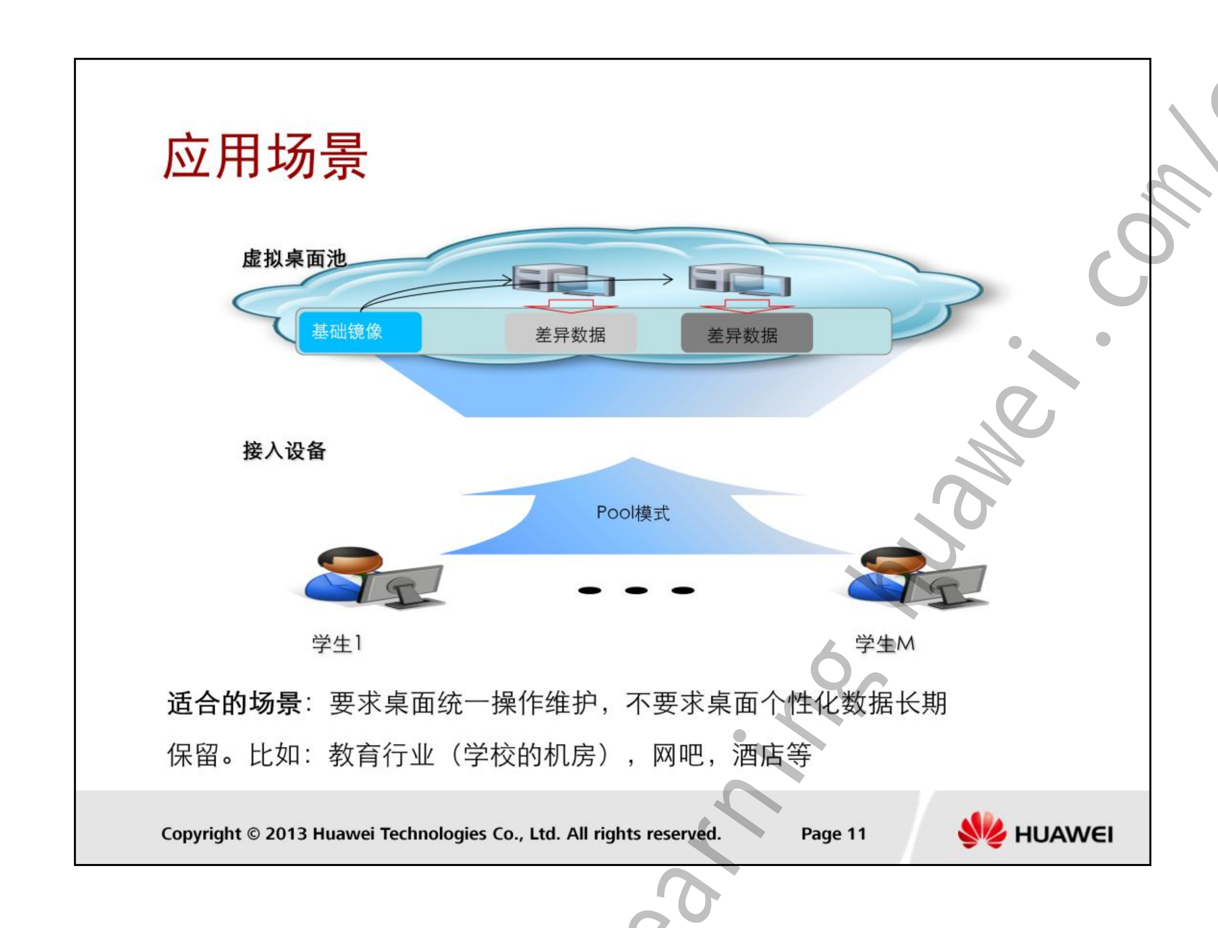


- M:N分配方式：用户与虚拟机没有固定的绑定关系，但一个用户一次只能使用其中一台虚拟机。
- 1:1分配方式：一台虚拟机可以分配给多个用户，但首次使用时会绑定给固定用户，且一个用户只能绑定一台虚拟机。
- PvD静态池类型的桌面组：Personal virtual Disk是面向虚拟桌面的一种个性化解决方案。PvD保留了池桌面和流桌面的单映像管理功能，同时允许用户安装应用程序和更改自己的桌面设置；它将对用户VM所做的更改重定向到连接至用户VM的独立磁盘（即个人虚拟磁盘），从而将每位用户的个性化设置分隔开来。个人虚拟磁盘中存储的内容在运行时与基础VM（母卷及差分卷所呈现的系统盘）中的内容混合在一起，以提供一致的体验。PvD静态池桌面组，简单地说就是静态池模式发布桌面还可以个性化安装各自的软件，并且主镜像（母卷）更新后也不影响更新之前用户安装的软件。

链接克隆桌面池

桌面池类型	特点
动态池	• M:N分配方式（用户与虚拟机没有固定的绑定关系，但一个用户一次只能使用其中一台虚拟机） • 默认有关机自动还原功能 • 适用于任务型桌面（个性化数据不保存）
静态池	• 1:1分配方式（一台虚拟机可以分配给多个用户，但首次使用时会绑定给固定用户，且一个用户只能绑定一台虚拟机） • 默认无关机自动还原功能 • 母卷系统更新或还原时，用户数据和用户安装的软件会丢失 • 适用于任务型桌面（一段时间内保存个性化数据）
PvD静态池	• 1:1分配方式 • 默认无关机自动还原功能 • 母卷系统更新或还原时，用户数据及用户安装的软件能最大程度不受到影响 • 适用于个性化较强，安全性要求不高，个性化数据偶尔丢失掉也能接受，有统一桌面维护能力的场景





场景特点：

- 虚拟机重启后还原初始状态
- 所使用的软件经常需要更新
- 用户数量多，存储需求量大
- 学习资料要求有单独空间保存

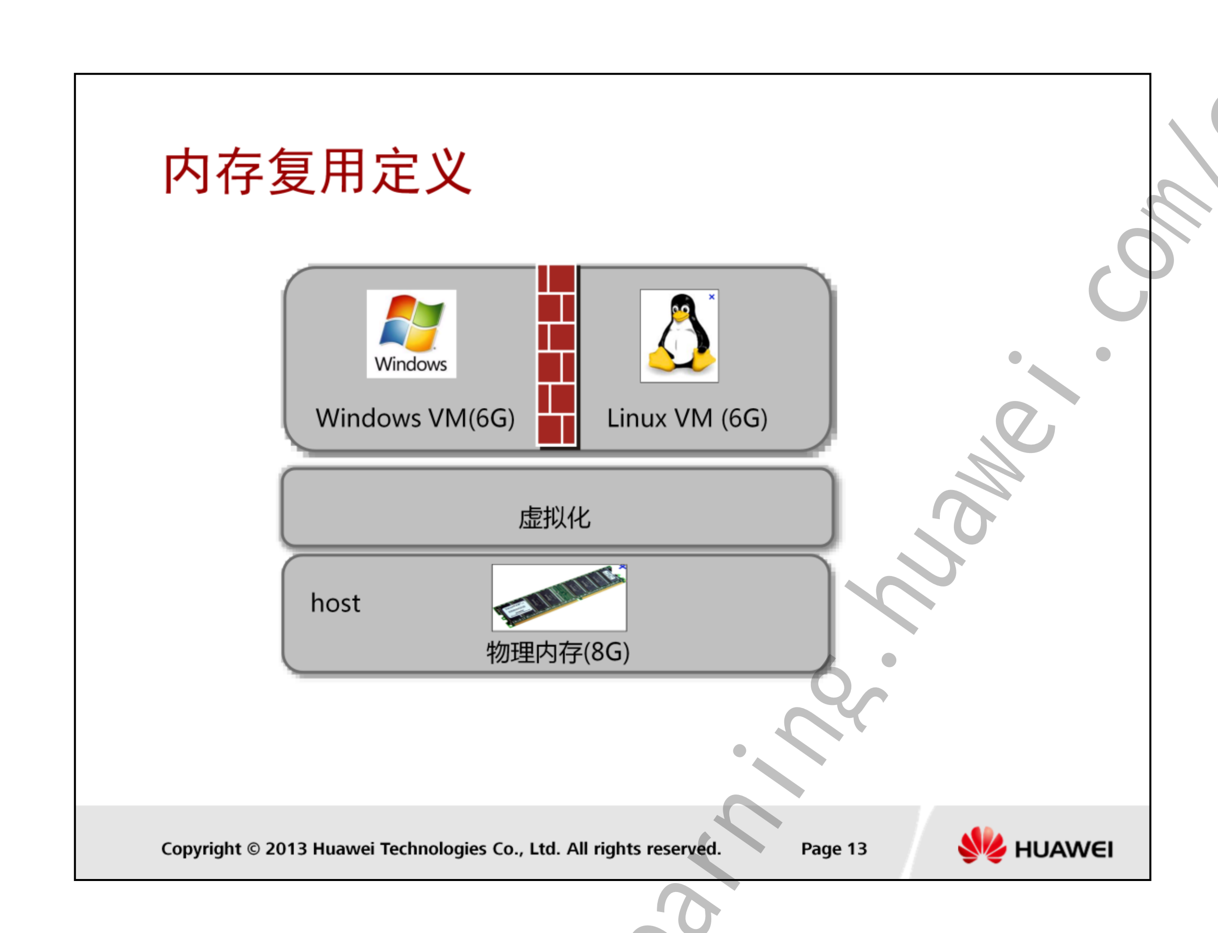
链接克隆方案：

- 通过Golden image方便地增加或更新所有学生用机上的软件
- 每个虚拟机只在存储上保存修改部分的内容，节约存储空间
- 学生注销桌面后，虚拟机自动恢复原始状态
- 每个学生分配一定的网络存储空间（如NAS网盘），用于保存个人资料



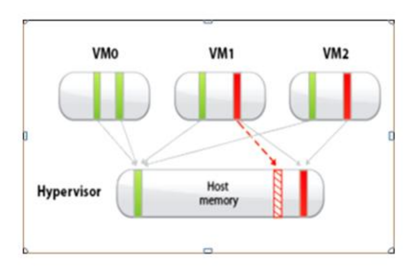
目录





内存复用：通过虚拟化技术，在同一主机上运行的虚拟机内存规格总和大于主机内存规格，从而在不增加物理内存的情况下，提高虚拟机密度，降低单台虚拟机成本。并且针对不同虚拟机（例如，管理虚拟机），提供不同QoS（服务质量），满足客户的业务需求。

透明页共享



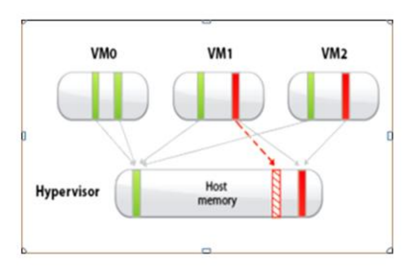
- 当主机内存使用量超过阈值时，可以自动将主机上的多个虚拟机使用的内容一样的多个内存页在物理机内存中进行合并，从而释放出物理内存，供更多的虚拟机使用
- 通过内存透明页共享技术，可以更高效地使用物理服务器的内存资源，并允许在相同配置下运行更多的虚拟机

 Page 14



- 注：目前FusionCompute只实现了零页共享技术，对于透明页共享暂时没有实现

零页共享

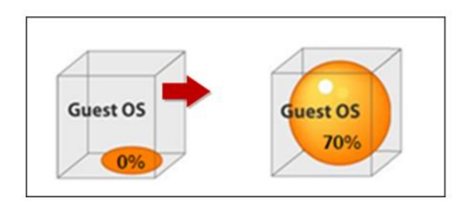


- 当主机内存使用量超过阈值时，可以自动将主机上的多个虚拟机的零页内存在物理机内存中进行合并，释放出更多的物理内存供虚拟机使用



- 注：零页共享只是透明页的一种特例

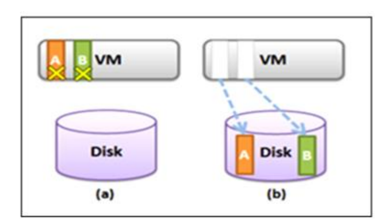
内存气泡



- 当虚拟机内存压力较小时，利用虚拟机中的前端驱动程序，将虚拟机的空闲内存提供给主机，可以释放出更多的物理内存供虚拟机使用
- 内存气泡技术在操作系统感知虚拟机内存使用量下使用，对虚拟机性能影响较小，但是在内存减少时，用户能感知到



内存交换

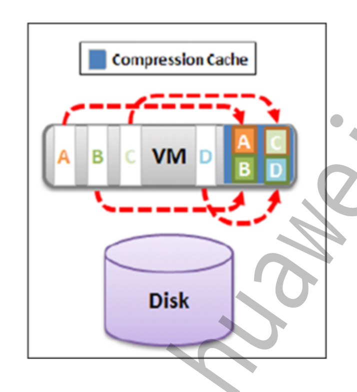


- 当虚拟机内存压力较大时，将虚拟机的内存页交换到磁盘中从而释放内存
- 当虚拟机内存页交换到磁盘后，虚拟机的性能将下降比较明显



内存压缩

- 虚拟机开辟一段空间，在交换前先进行内存压缩，尽可能减少内存交换
- 通过内存压缩，减少了虚拟机内存交换，提高虚拟机的性能。



 Page 18



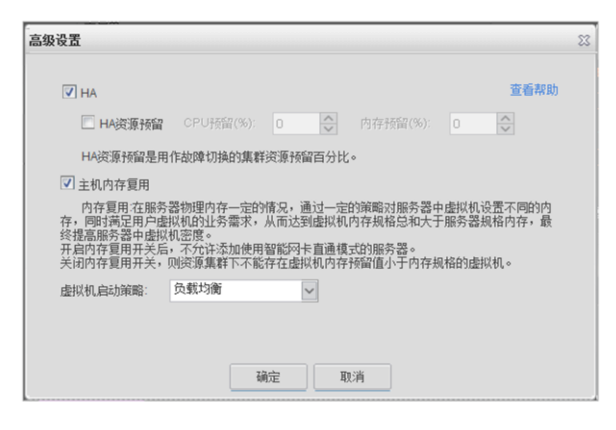
- 内存压缩技术的主要思想是将数据按照一定的算法压缩后存入压缩内存中，系统从压缩内存中找到压缩过的数据，将其解压后即可以供系统使用。这样既可以增加实际可用的内存空间，又可以减少页面置换所带来的开销，从而以较小的成本提高系统的整体性能。

内存策略

- 使用各种内存复用技术(内存气球、零页共享和内存交换)，通过合理的调度，使主机上的虚拟机对内存的访问及时响应，减少内存复用开启情况下虚拟机性能损耗。



内存复用参数



- 内存复用开关
  - 对象为站点下集群，通过高级设置对集群下主机决定是否打开内存复用开关，默认情况关闭内存复用开关
  - 内存复用开关关闭情况下，主机内存复用不生效

 Page 20



- 注：主机内存复用与HA资源预留、虚拟机启动策略等无任何关系，以上三者均是集群的高级属性。

内存复用参数



- 内存QoS
  - 对象为虚拟机，QoS参数包括内存预留、内存份额和内存限额
  - 内存预留表示虚拟机的最小使用量，如下图，虚拟机内存规格为4096M，内存预留0M
  - 内存份额表示主机内存不足情况下，虚拟机获得内存的权重。如下图，虚拟机的份额为中，即虚拟机内存大小乘10为40960
  - 内存限额表示虚拟机的最大使用量。内存限额为内存规格4096M



- 注意：

(1) 只有在主机满足虚拟机预留的情况下，才会允许启动虚拟机

(2) 只有在主机内存不足的情况下，内存份额才会生效

(3) 内存限额同虚拟机规格

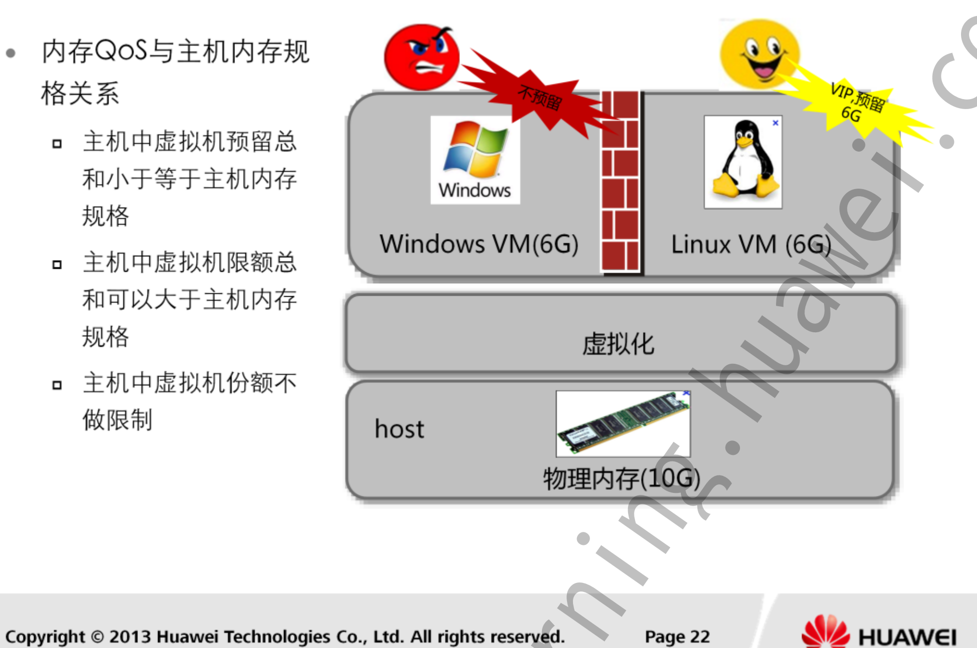
举例说明：

一个主机有4G内存，上面运行2个3G内存虚拟机，预留都是1G；这样主机中4G内存，至少有1G是虚拟机1，另外1G给虚拟机2，剩余2G内存按需分配给虚拟机1和虚拟机2。如果虚拟机1需要1G内存，虚拟机2需要3G内存，这样虚拟机1靠预留的1G内存就满足业务了，而虚拟机2需要预留的1G+主机剩余的2G内存。 但是，如果虚拟机1和虚拟机2都需要3G，主机的剩余2G内存不满足虚拟机业务需求，这时需要通过份额分配这2G内存。

假如虚拟机1的份额是2000，而虚拟机2的份额是1000，根据份额的权重：

虚拟机1获取的内存=预留的1G＋(2000/（2000+1000）)*2G＝1＋1.33=2.33；

虚拟机2获取的内存=预留的1G＋(1000/（2000+1000）)*2G＝1＋0.67=1.67。


虚拟机QoS与主机内存关系
内存QoS与主机内存规格关系
主机中虚拟机预留总和小于等于主机内存规格
主机中虚拟机限额总和可以大于主机内存规格
主机中虚拟机份额不做限制
不预留
VIP,预留 6G
Windows
Windows VM(6G)
Linux VM (6G)
虚拟化
host
物理内存(10G)
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 22
HUAWEI



目录

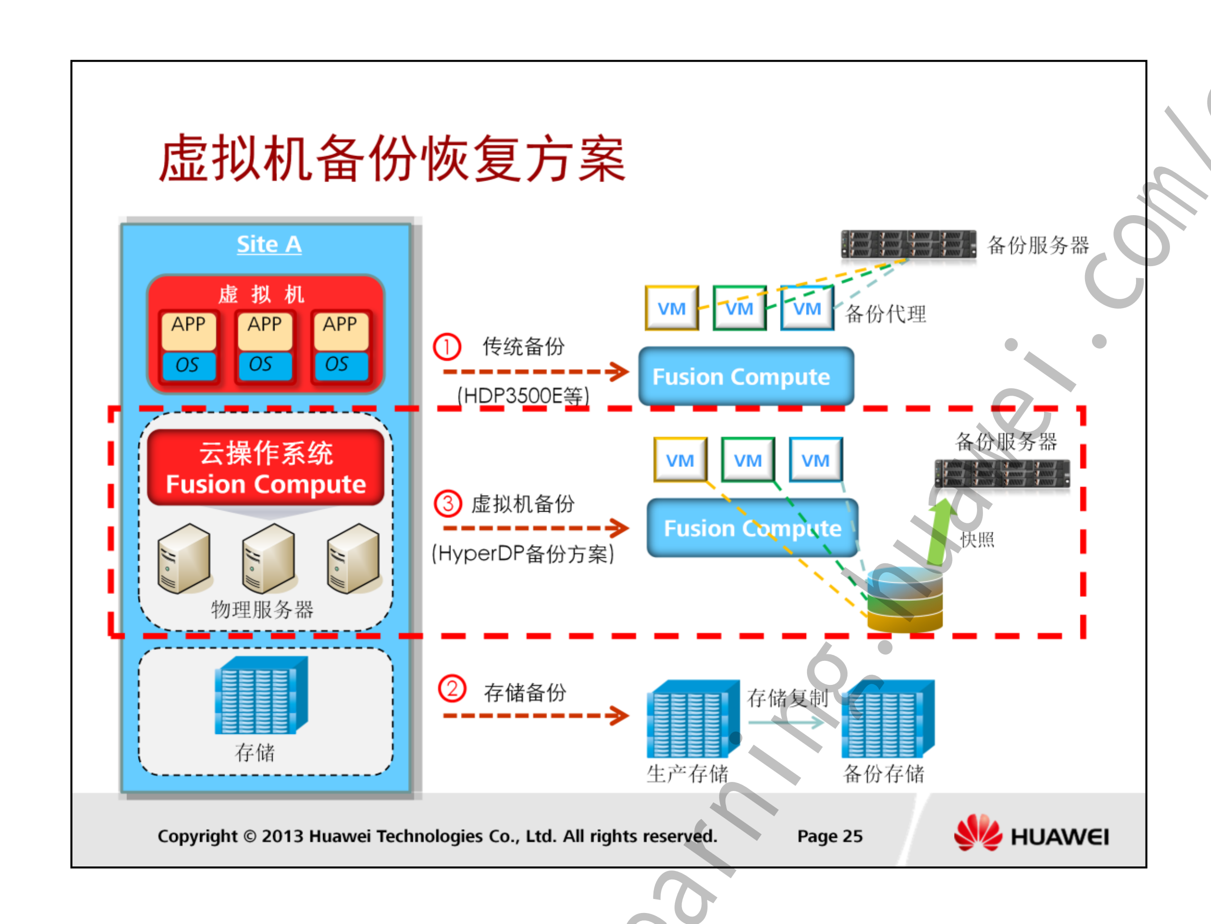


为什么需要备份恢复

- 服务器宕机、网络设备故障、存储设备损坏等物理设备故障造成数据丢失
- 软件BUG、病毒及误删除、非正常关机等人为误操作造成数据丢失
- 火灾、水灾、地震等灾难引发站点故障而造成数据丢失







1、传统备份：在每个需要备份的虚拟机内安装备份代理软件，通过备份代理将虚拟机数据备份到备份服务器上；

主要缺点：需要在虚拟机内安装备份代理，安装部署复杂；只能针对应用数据进行备份和恢复，无法对操作系统和软件进行备份恢复

2、存储备份：利用存储复制功能，将生产存储上某些LUN数据复制到备份存储同样大小的LUN上，在主存储故障时可使用备存储快速接管业务

主要缺点：要求生产存储与备份存储为同一厂家设备；只有虚拟机位于复制LUN上时才能备份，无法针对单个虚拟机做备份

3、虚拟机备份：以虚拟机为对象进行备份，不需要安装备份代理，可备份和恢复虚拟机的系统卷和数据卷。

虚拟机备份恢复方案汇总

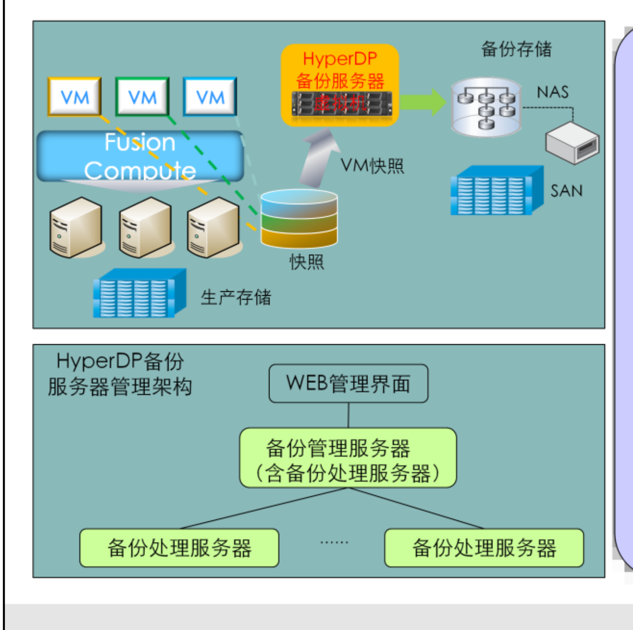
类型	方案描述	主要应用场景	约束	我司方案
虚拟机备份	针对虚拟机快照的备份	1、针对虚拟机或卷的备份 2、针对系统卷与数据卷的备份与恢复	1、不能针对虚拟机内文件备份 2、只支持备份到磁盘 3、恢复数据量大，恢复时间长	HyperDP虚拟机快照备份
传统备份	针对虚拟机内文件或目录的备份	1、支持应用级别的备份 2、支持备份到磁带库	1、每个虚拟机上需要安装一个备份代理 2、虚拟机开机时才能备份 3、无法恢复系统卷	1、存储产品HDP3500E备份设备 2、NAS网盘备份
存储备份	针对存储的备份	1、针对批量虚拟机系统卷与数据卷的备份与恢复 2、生产存储故障时快速恢复业务	1、基于Lun级别备份，而非虚拟机 2、无法保证数据的一致性 3、备份存储必须与生产存储同构，且按1:1配置	1、利用阵列复制功能备份 2、存储采用NAS时，利用NAS复制功能备份

 Page 26



- 利虚拟机备份：用云平台虚拟机快照功能，由HyperDP定期将虚拟机快照备份到NAS/SAN上
- 不需要在VM内安装备份代理软件
- 不需要终端用户参与，备份与恢复操作均由系统管理员完成

HyperDP虚拟机备份方案总体介绍



HyperDP虚拟机备份

1、**简单易用**：无需安装备份代理，备份服务器通过虚拟机模板安装，通过浏览器即可进行管理

2、**灵活备份策略**：支持周期性全量与增量备份策略，可灵活设置备份周期与备份时间窗口，支持备份数据过期策略以自动清理过期备份数据，并可针对不同类型VM设置不同备份策略

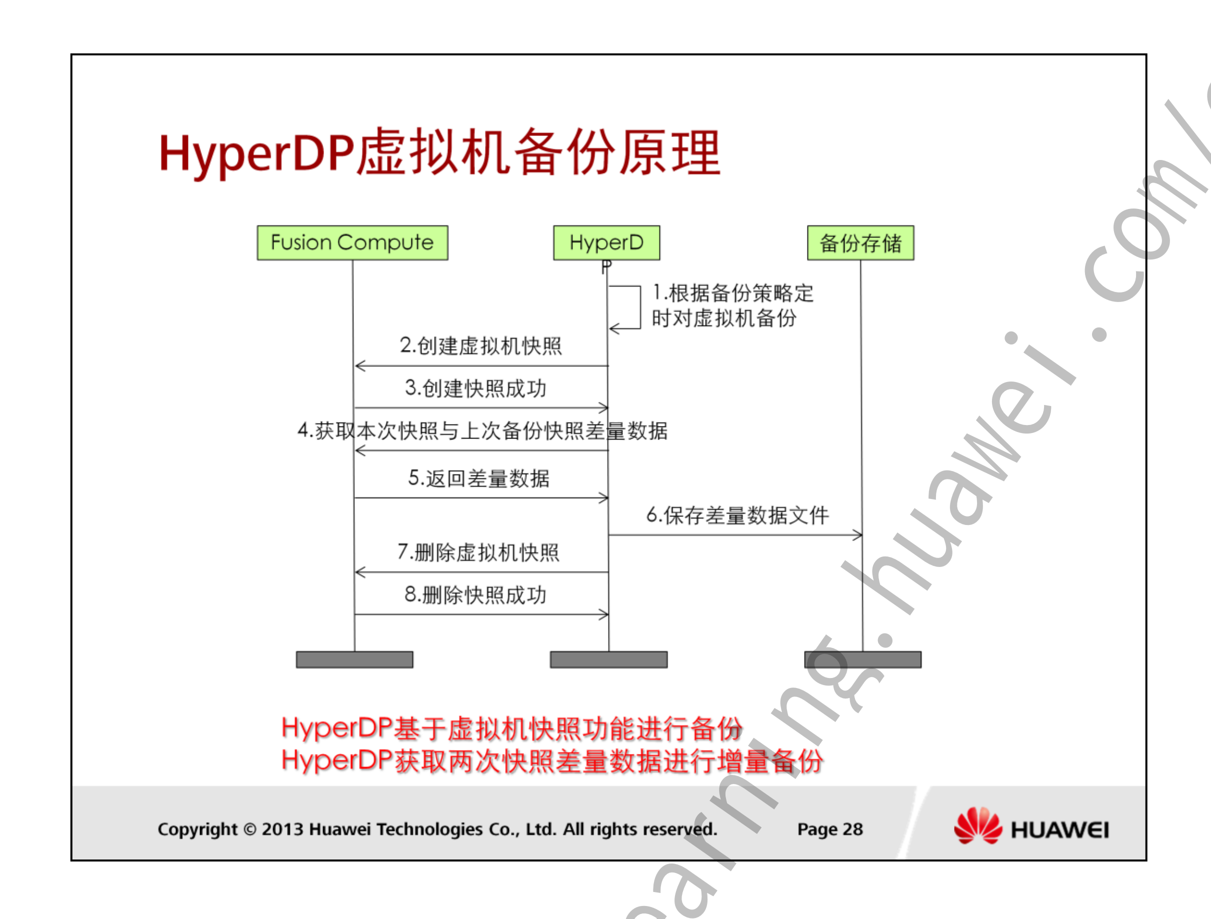
3、**高效备份与恢复**：全量备份时只备份有效数据，增量备份时只备份非重复更改数据，减少无效数据备份，最大限度减少备份通信流量与备份存储空间需求

4、**并发备份与恢复**：每个设备最多支持8个VM并发备份与恢复，每个备份域支持10个备份服务器，可进行统一管理；由于HyperDP 位于专用虚拟机上，备份处理对生产VM基本没有影响

Page 27



- HyperDP：Hyper Data Protection
- 备份域：一个备份管理服务器及其管理的所有备份处理服务器组成一个备份域
- HyperDP虚拟机与NAS之间为NFS/CIFS网络文件共享协议，HyperDP将NAS上共享目录作为备份的目的目录
- HyperDP虚拟机使用SAN作为备份存储时，需要从SAN所在数据存储上创建虚拟磁盘，挂载给HyperDP所在虚拟机，作为备份存储
- HyperDP虚拟机通过业务平面访问FusionComputer、NAS，生产存储为FusionStorage时通过存储平面访问FusionStorage



- 备份业务流程描述如下:

1、HyperDP保存虚拟机备份策略，并检测备份策略是否到期;

2、HyperDP发现备份策略到启动时间，选择要备份的目标VM，向VM所属Fusion Compute发送创建快照消息，消息携带虚拟机标识;

3、Fusion Compute收到消息后，对VM创建新的快照，返回新创建的快照标识给HyperDP ;

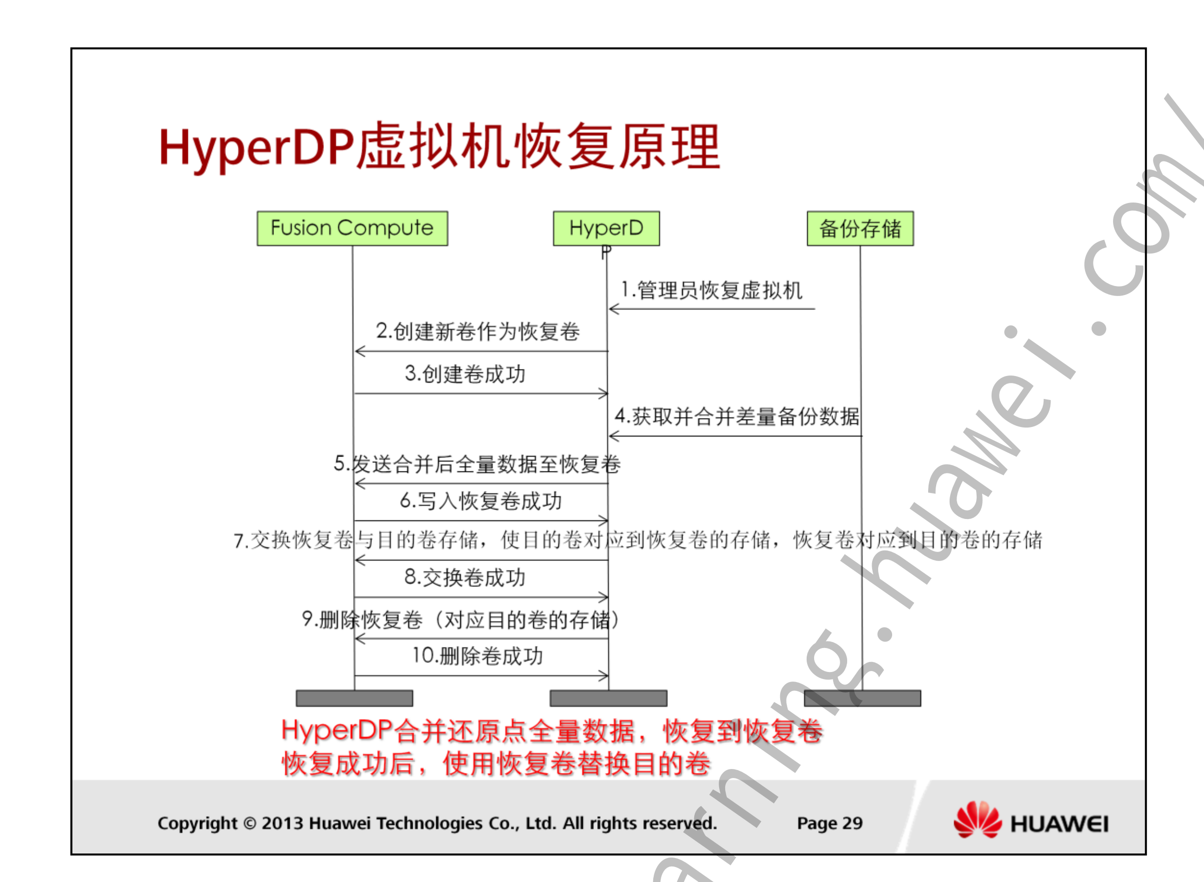
4、当需要差量备份时，HyperDP请求获取本次快照与上次快照之间的差量数据；对于全量备份，HyperDP请求获取本次备份快照的全量数据;

5、FusionCompute收到消息后，将备份数据返回给HyperDP;

6、HyperDP将备份数据保存到备份存储中。 备份存储可以是备份处理服务器的本地存储，也可以是外接的NAS存储;

7、备份完成后，HyperDP删除备份所产生的虚拟机快照;

8、FusionCompute删除为备份产生的虚拟机快照。



- 数据恢复业务流程描述如下：

1、某个虚拟机或卷需要恢复时，管理员创建恢复任务；

2、HyperDP向VM所属FusionCompute发送创建恢复卷消息，用于保存恢复数据；

3、FusionCompute收到消息后，创建恢复卷，返回创建成功消息给HyperDP；

4、HyperDP从备份存储中获取需要恢复的文件并进行合并；

5、HyperDP向FusionCompute发送恢复全量数据；

6、FusionCompute收到恢复数据后写入恢复卷，并返回成功；

7、卷所有数据都上传并写入到恢复卷后，HyperDP通知FusionCompute交换恢复卷与旧的存储卷与存储的对应关系，使原卷对应到新恢复卷的存储，新卷对应到原卷的存储；

8、FusionCompute交换新卷与原卷的对应存储，向HyperDP返回成功消息；

9、HyperDP通知FusionCompute删除新恢复卷（对应原卷的存储）；

10、FusionCompute删除新恢复卷。

- 先恢复到恢复卷的目的：直接恢复到目的卷时，可能会出现恢复过程中恢复失败，导致目的卷数据完全破坏的情况；先恢复到恢复卷，可避免恢复过程中出现异常；缺点是：恢复卷需要额外占用存储空间，需要保证恢复目的存储上有足够空间进行恢复。

备份服务器安装部署和管理

- 备份服务器虚拟机安装:
  - 模板方式
  - ISO包方式
- 备份服务器配置
  - 通过VNC登录
  - 执行脚本配置服务器类型（管理、处理）、生产存储类型（FusionStorage、虚拟存储）、网络信息（IP地址等）
- 备份服务器管理:
  - 查看备份服务器
  - 注册备份服务器以加入备份域
  - 删除备份服务器
  - 修改备份服务器网口信息
  - 查看备份服务器拓扑结构
  - 备份服务器的灾难恢复



备份 > 系统管理 > 备份服务器

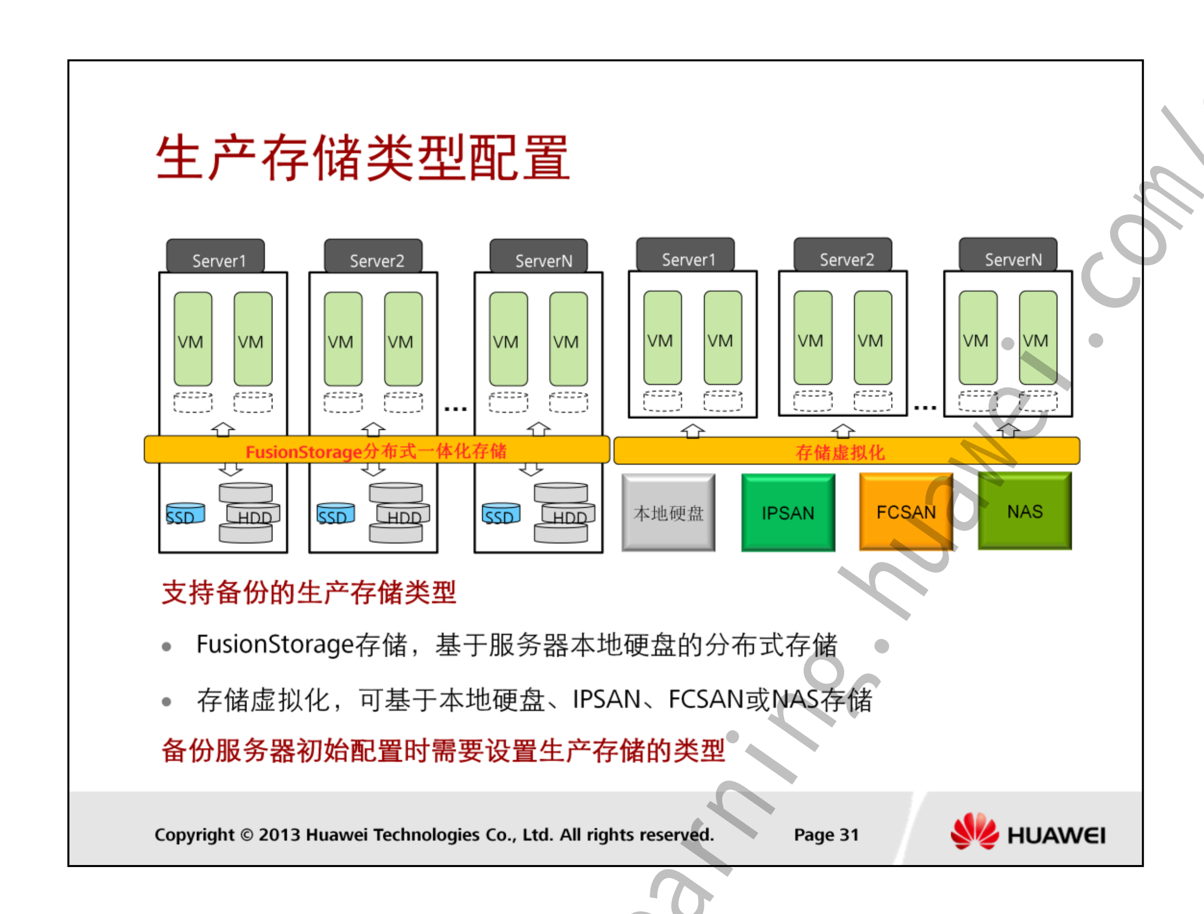
备份服务器列表

注册 删除

	ID	名称	角色	状态	IP地址	受保护的虚拟机数	备份域
●	1	dps4	备份管理服务器	在线		7	已注册
○	2	DPS05	备份处理服务器	离线	192.168.20.65	0	已注册

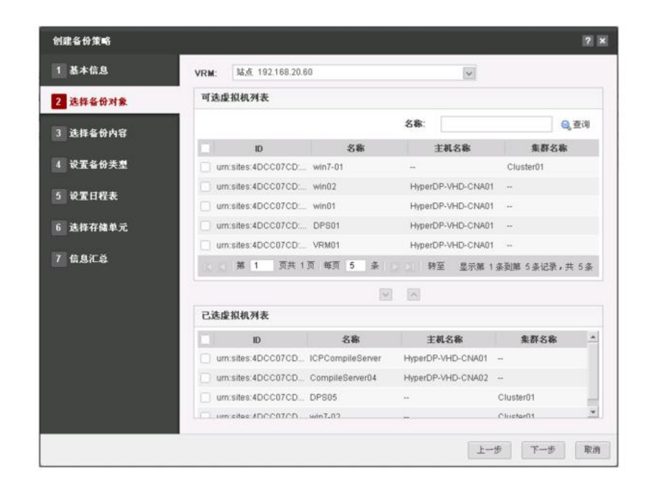
第 1 页共 1 页 | 每页 10 条 | 转至　　显示第 1 条到第 2 条记录，共 2 条

HUAWEI



- 对于FusionStorage存储，HyperDP通过FusionStorage存储平面进行备份
- 对于存储虚拟化，HyperDP通过管理平面进行备份

灵活备份策略 – 备份对象



- 单个虚拟机
- 虚拟机批量备份



灵活备份策略 – 备份内容



- 整个虚拟机
- 虚拟机某几块磁盘



灵活备份策略 – 备份类型



- 完全备份
- 完全备份 + 增量备份



灵活备份策略 – 调度计划



选择备份调度周期

- 可对完全备份与增量备份分别设置备份周期
- 按周、按月和指定周期备份



选择备份时间窗口

- 指定备份开始时间
- 指定备份持续时间

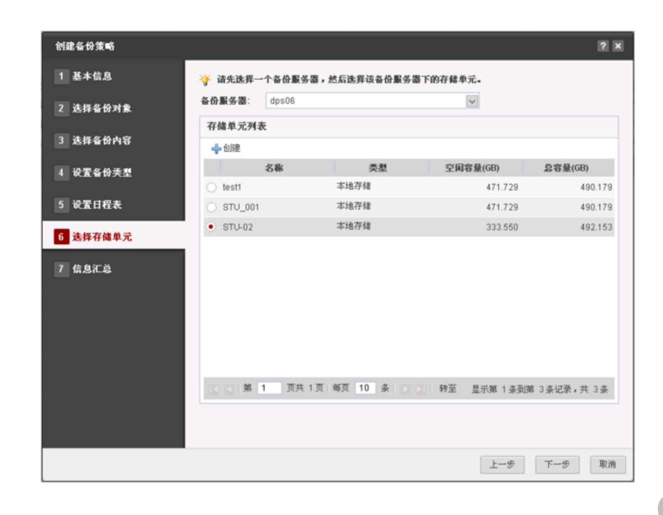
选择备份数据过期策略

- 指定时间，选择几天、几周或几月

HUAWEI



灵活备份策略 – 存储单元



选择备份存储单元

- NFS共享存储
- CIFS共享存储
- 备份服务器本地存储（指挂载给备份服务器虚拟机的虚拟磁盘）

 Page 36



- NFS（Network File System）,网络文件系统是FreeBSD支持的文件系统中的一种，也被称为NFS。NFS允许一个系统在网络上与他人共享目录和文件。通过使用NFS，用户和程序可以像访问本地文件一样访问远端系统上的文件。
- CIFS（Common Internet File System)，通用Internet文件系统，CIFS使程序可以访问远程Internet计算机上的文件并要求此计算机的服务。CIFS 使用客户/服务器模式。客户程序请求远端服务器上的服务器程序为它提供服务。服务器获得请求并返回响应。CIFS是公共的或开放的SMB协议版本，并由Microsoft使用。SMB协议现在是局域网上用于服务器文件访问和打印的协议。象SMB协议一样，CIFS在高层运行，而不象TCP/IP协议那样运行在底层。CIFS可以看做是应用程序协议如文件传输协议和超文本传输协议的一个实现。
- CIFS 可以使您达到以下功能：
  - 1.访问服务器本地文件并读写这些文件
  - 2.与其它用户一起共享一些文件块
  - 3.在断线时自动恢复与网络的连接
  - 4.使用统一码（Unicode）文件名：文件名可以使用任何字符集，而不局限于为英语或西欧语言设计的字符集。
- 一般来说，CIFS使用户得到比FTP更好的对文件的控制。它提供潜在的更直接地服务器程序接口，这比使用HTTP协议的浏览器更好。CIFS最典型的应用是windows用户能够从“网上邻居”中找到网络中的其他主机并访问其中的共享文件夹。

备份策略执行



策略名称	备份内容	备份服务器	备份类型	优先级	存储单元	备份集保留时间	状态	创建时间
test	整机	--	完全备份	5级	test123777	1周	启用	2013-03-01 15:49:...
backup-001	硬盘	--	差异增量式备份	1级	stu-109	永久保存	启用	2013-03-01 16:06:...
backup	整机	--	完全备份	5级	ateawy	1周	启用	2013-03-01 16:07:...
backup-server	--	--	完全备份	--	--	5天	启用	2013-03-01 16:30:...
backup00001	整机	--	完全备份	5级	stu-111	4周	启用	2013-03-01 16:38:...
luo-1	--	--	完全备份	--	--	1天	启用	2013-03-01 17:02:...
luo-2	硬盘	--	差异增量式备份	9级	stu-i	1周	启用	2013-03-01 17:05:...
wwq	--	--	完全备份	--	--	1周	启用	2013-03-04 21:33:...

- 自动执行备份任务
- 手动启动立即执行备份



备份作业管理



监控 > 作业信息 > 备份作业

备份作业列表

删除 取消 策略名称 查询 高级查询

ID	作业类型	备份类型	策略名称	状态	进度	源VRM名:	源VRM IP	虚拟机名:	备份内容	磁盘槽位:	备份服务:	存储单元	速率	开始时间	结束时间
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-20	2013-03-20
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-20	2013-03-20
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-20	2013-03-20
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-20	2013-03-20
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-20	2013-03-20
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-20	2013-03-20
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-20	2013-03-20
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-20	2013-03-20
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-19	2013-03-19
100000000:	自身灾备	完全备份	backup-001	失败	--	--	--	--	--	--	dps4	--	0M/s	2013-03-19	2013-03-19

第 1 页共 4 页 每页 10 条 转至 显示第 1 条到第 10 条记录，共 39 条

- 查看备份作业状态
- 查询备份作业
- 取消备份作业
- 删除备份作业

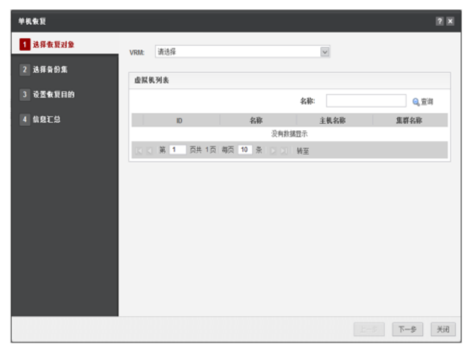


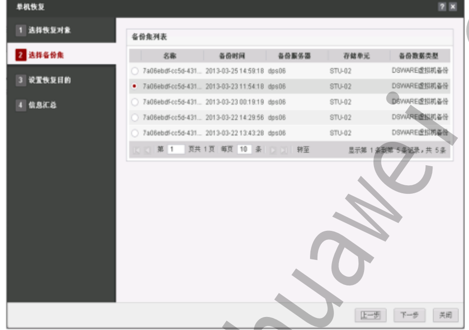
备份集管理

- 查询备份集
  - 可以查看备份域中所有备份集的信息，或者按指定的条件查询备份集的信息
- 修改过期策略：
  - 当备份集的保留时间需求改变时，可以修改备份集的过期策略
- 导入备份集
  - 当备份服务器故障时，将存储单元中存在但备份服务器无法识别的备份集导入备份域，从而可以使用该备份集



恢复任务设置 – 备份集选择





选择恢复源

- 选择备份虚拟机
- 选择指定时间点备份集



恢复任务设置－恢复目的选择



- 支持单机和批量磁盘恢复到原虚拟机
- 支持单机和批量整机恢复到新创建虚拟机
- 支持单机磁盘恢复到指定其他虚拟机



恢复作业管理



监控 > 作业信息 > 恢复作业

恢复作业列表

删除 取消 状态 全部 查询 高级查询

ID	恢复类...	状态	进度	虚拟机名称	备份服务器	存储单元	速率	目的VRM...	目的VRM ...	目的虚拟...	开始时间	结束时间
aa92b8bd-f99...	整机	已取消	--	VM088039c6-...	backup001	--	0M/s	--	--	huhu	2013-01-31 1...	--
dbcd825b-02...	整机	正在等待	--	VM088039c6-...	backup001	--	0M/s	--	--	huhuhu	2013-01-30 1...	--
d2d59027-ba...	整机	成功	--	VM088039c6-...	backup001	--	0M/s	--	--	HUHU	2013-01-30 1...	--
273efac8-6e4...	整机	失败	--	VM088039c6-...	backup001	--	0M/s	--	--	HUHU	2013-01-30 1...	--
bcc9cef5-160...	整机	已取消	--	VM088039c6-...	backup001	--	0M/s	--	--	HUHU	2013-01-30 1...	--
273e2c8-6e4...	整机	成功	--	VM088039c6-...	backup001	--	0M/s	--	--	HUHU	2013-01-30 1...	--
bcc9cef5-123...	整机	失败	--	VM088039c6-...	backup001	--	0M/s	--	--	HUHU	2013-01-30 1...	--
d2d59027-ba...	整机	正在等待	--	VM088039c6-...	backup001	--	0M/s	--	--	HUHU	2013-01-30 1...	--
273efac8-6e4...	整机	已取消	--	VM088039c6-...	backup001	--	0M/s	--	--	HUHU	2013-01-30 1...	--
bcc9cef5-160...	整机	正在运行		VM088039c6-...	backup001	--	0M/s	--	--	HUHU	2013-01-30 1...	--

第 1 页共 5 页 每页 10 条 转至 显示第 1 条到第 10 条记录，共 44 条

- 查看恢复作业状态
- 查询恢复作业
- 取消恢复作业
- 删除恢复作业



关键规格

项目	规格
每台备份服务器备份虚拟机的数量	200台
一个备份域中支持的备份服务器数量	10台
一个备份域中备份虚拟机的数量	2000台
每台备份服务器支持并发备份恢复流的数量	8
一个备份域中备份策略的数量	200
一个备份域中存储单元数量	10000





目录

1. 云计算技术概述
2. 链接克隆
3. 内存复用
4. 备份和恢复
5. **虚拟机快照**
6. 虚拟机迁移
7. 虚拟机资源在线调整
8. 动态资源调度



快照的概念

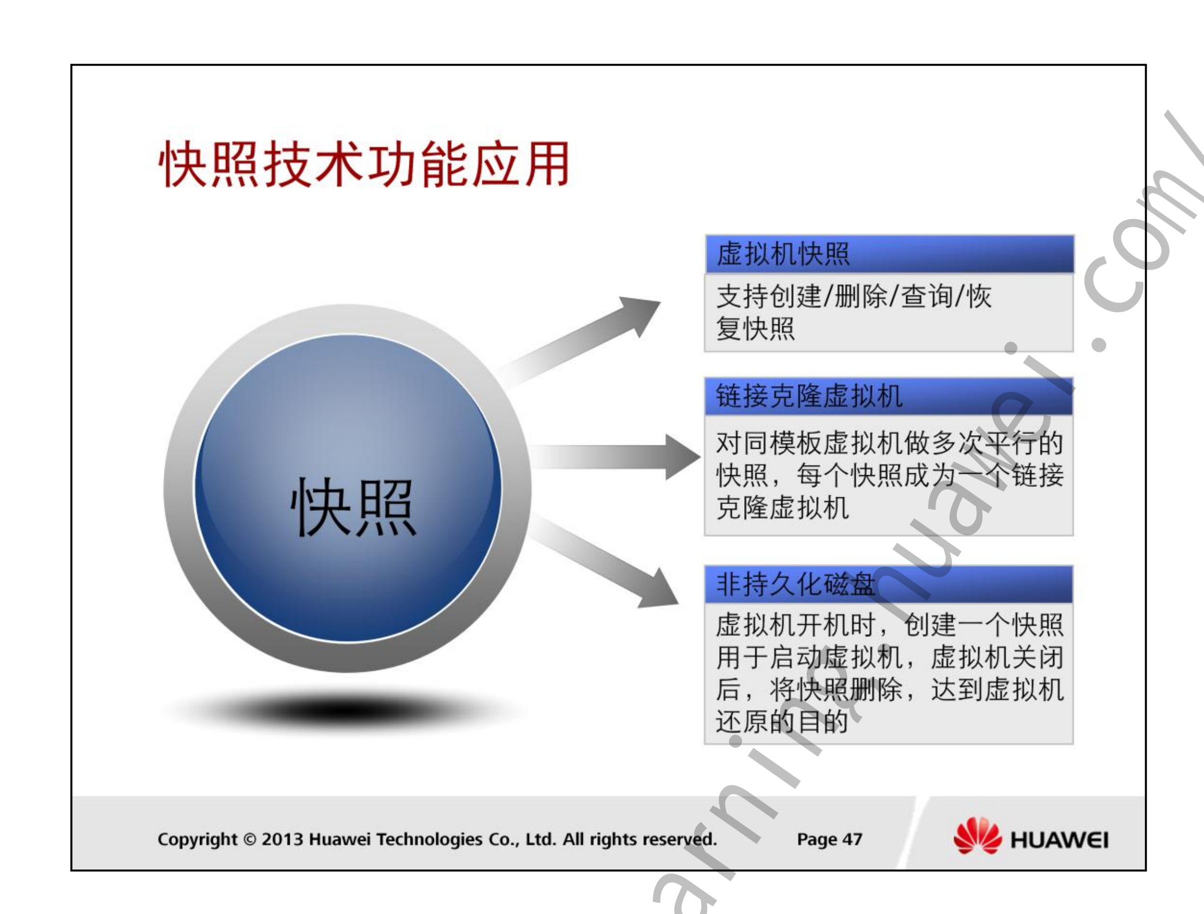
- 什么是快照
  - 快照记录了虚拟机磁盘文件在某一时间点的内容
  - 通过执行虚拟机快照保存虚拟机在某一点的状态
  - 通过恢复虚拟机快照使虚拟机快速恢复到某一时间点的状态
  - 快照包含磁盘内容、虚拟机配置信息、内存数据
- 快照的应用
  - 虚拟机用户在执行一些重大、高危操作前，例如系统补丁，升级，破坏性测试前执行快照，可以用于故障时的快速还原



快照的作用和价值

- 客户痛点：
  - 重大操作前进行数据备份，耗时太久
  - 所有数据备份需要占用大量存储空间
  - 每一次备份恢复耗时太久
- 解决策略
  - 每次快照保留差异化信息，可以使用尽量少的存储空间前提下，保存快照点用户数据的所有状态。
  - 快照的创建和恢复均为低时延操作，用户无需等待



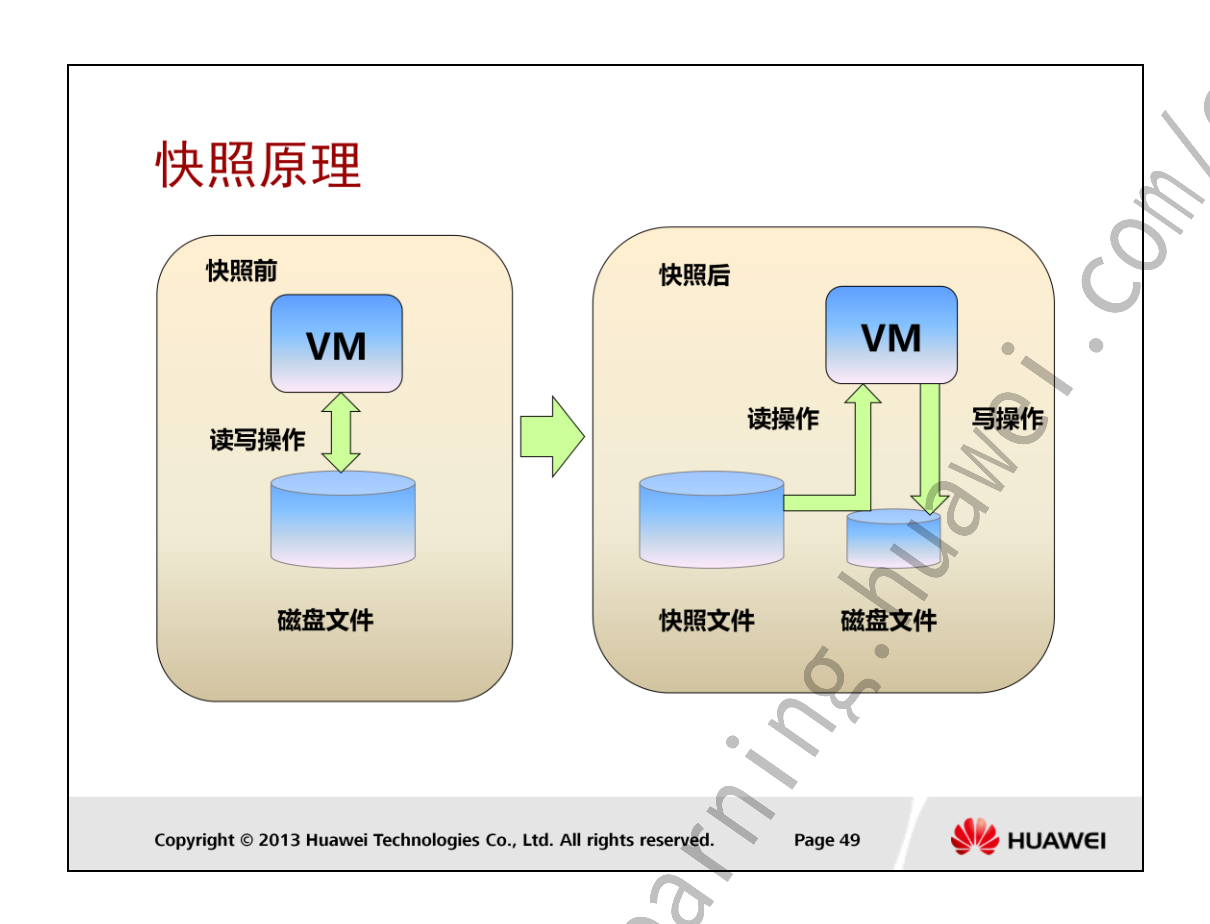


- 本节描述了快照技术的具体应用:
  - 虚拟机快照功能包括了快照创建、删除、恢复、查询等操作。
  - 链接克隆虚拟机技术是针对一个链接克隆模板（系统磁盘），生成一个链接克隆母卷，再对这个母卷做多次快照，每个快照的差异文件都可以作为一个虚拟机的系统磁盘工作，读数据时会从差异文件+母卷获取，写数据时会保存在差异文件中，不影响母卷。
  - 非持久化磁盘功能是提供了虚拟机关机还原的业务，应用于网吧等公共计算机。虚拟机开机时，会自动创建一个快照的差异文件，将所有对磁盘的修改都写在差异文件中，关机后，该文件会被删除，虚拟机磁盘会还原到上次开机时的状态。

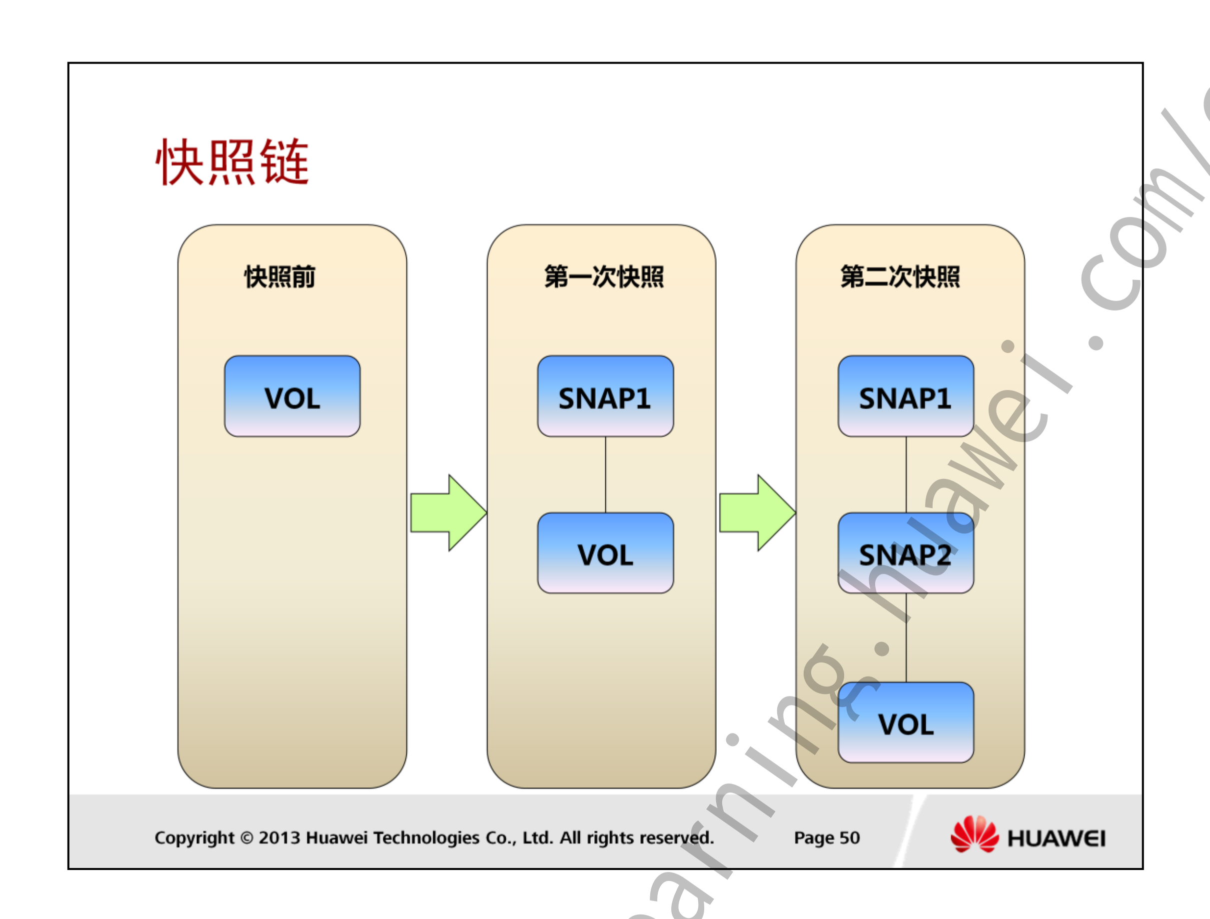
虚拟机快照

- 虚拟机快照包含虚拟机状态、虚拟机配置规格、所有磁盘数据、内存和寄存器数据（可选）
- 虚拟机磁盘不受快照参数影响，可以使该卷在做快照和恢复快照时数据不发生变化
- 磁盘快照根据不同的数据存储类型，原理不同：
  - 对于Advanced SAN存储和华为分布式共享存储，磁盘快照功能是由存储设备实现
  - 对于虚拟化存储，是由主机进行快照处理，后续章节主要基于这种快照技术进行讲解





- 执行虚拟机快照后，下列信息会被保存
    - 虚拟机的当前状态信息会被保存，例如CPU、内存数量，运行状态等信息
    - 虚拟机原来的的磁盘文件会变成只读的快照文件，以IO重定向的方式链接在一个新的磁盘文件上，用户新数据的写入会直接写在新磁盘文件上，而读取旧数据则会重定向到之前的磁盘文件（已经转为快照文件）。
    - 如果对运行中的虚拟机要求执行内存快照，则内存数据会保存在另一个文件中。



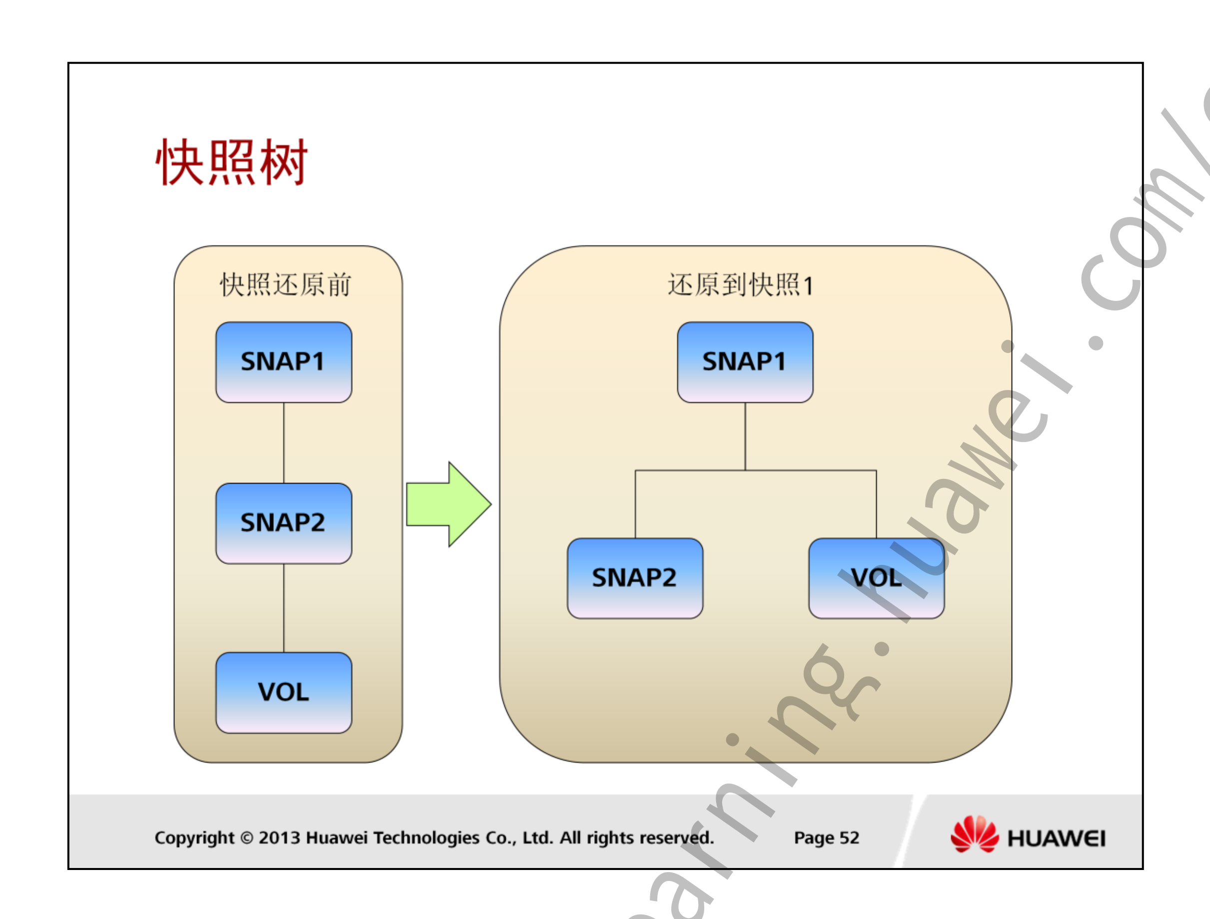
- 磁盘做多个快照后，会产生一个快照链
- 虚拟机卷始终挂载在快照链的最末端

从快照恢复虚拟机

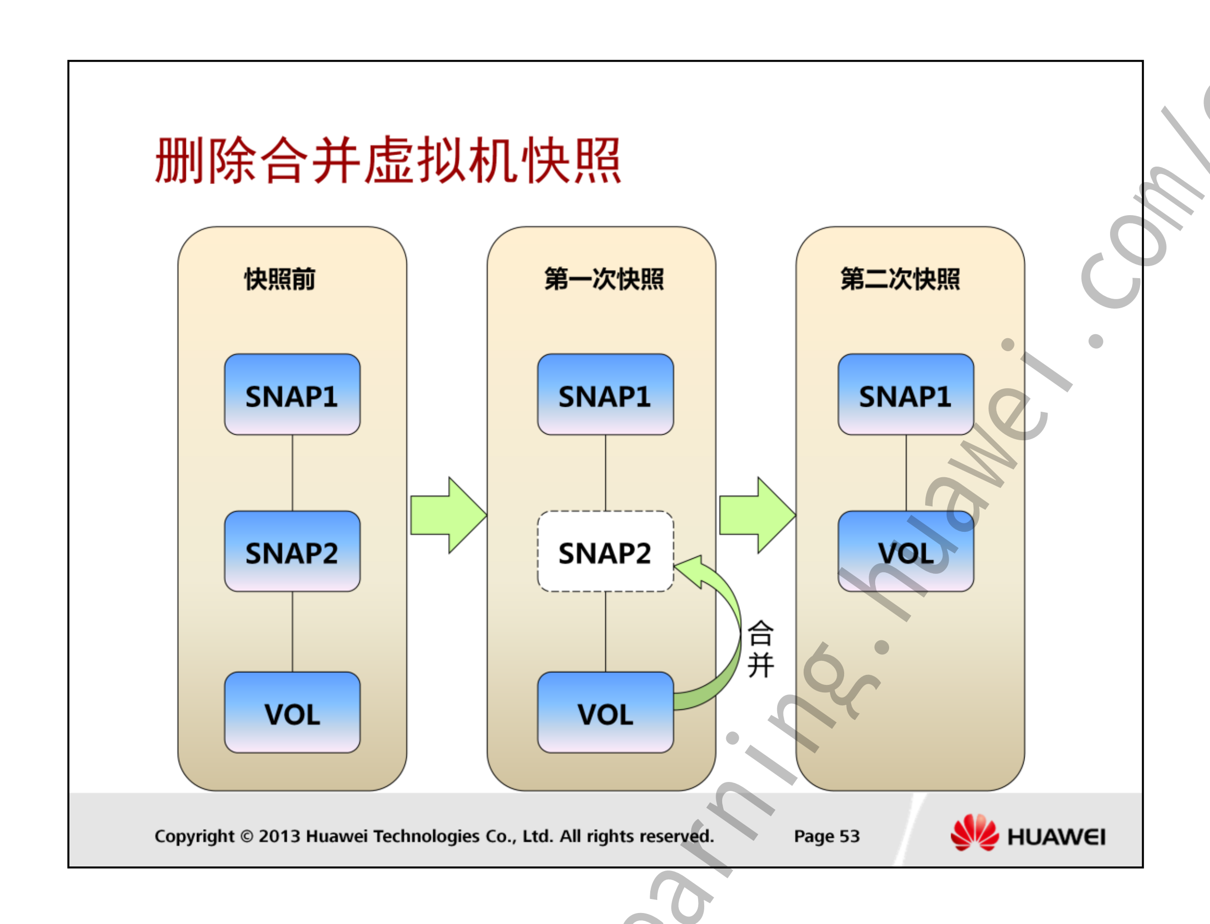
- 恢复快照可以使虚拟机快速回到快照点的状态
- 恢复快照时，会以虚拟机快照点为基准制作差分卷，使用这个差分卷启动虚拟机
- 原来虚拟机挂载的差分卷将被删除

警告！恢复快照会导致虚拟机在最后一次快照后的所有数据丢失！





- 快照链进行快照恢复虚拟机后，可能会产生快照树分叉
- 还原过程中，原先的卷（VOL）会被删除，然后创建新的VOL卷挂载给虚拟机使用。



- 删除快照通常会将此快照点将和它的子节点合并，成为新的子节点。
- 如果一个快照点有两个子节点，那么不会发生立刻合并，只有当其中一个子节点被删除后，才能被合并。



目录



虚拟机迁移

- 虚拟机迁移有两种方式:
- 虚拟机热迁移
  - 将运行中的虚拟机迁移至站点内指定的主机上
- 虚拟机存储迁移
  - 将虚拟机中的磁盘从一个数据存储迁移到另一个数据存储



虚拟机热迁移原理

- 将虚拟机配置和设备信息传送到目标主机上
- 传送虚拟机内存
  - 将虚拟机迁移时的初始内存及内存变更分片同步到目标主机上
- 暂停源虚拟机并传送状态
  - 在原主机上暂停虚拟机
  - 将最后的变更内存传到目标主机
- 恢复目标虚拟机
  - 在目标主机上恢复虚拟机，并在原主机上停止虚拟机

 Page 56



虚拟机存储迁移原理

- 存储冷迁移：
  - 在数据存储上拷贝磁盘文件
- 存储热迁移
  - 在目标数据存储上建立原卷的快照
  - 将虚拟机的IO切换到目标数据存储上的快照
  - 将原卷的数据块合并到目标数据存储的快照中
  - 删除原卷

 Page 57 



目录



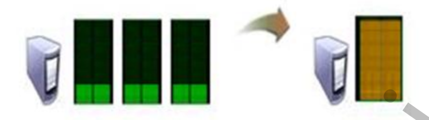
资源在线调整

- 虚拟机资源在线调整功能给客户提供计算资源的按需分配，提升计算资源的利用率
  - 当客户业务压力增加时可以获得更多的计算资源
  - 当客户业务压力减少时可以释放计算资源
- 包括虚拟机VCPU，内存，磁盘，网卡等资源在线调整



在线调整VCPU数量





管理程序监控虚拟机的资源压力情况，当出现计算资源CPU压力达到上限阀值时，通过调用VCPU热插拔来增加VCPU个数，从而缓解系统计算资源的压力

当系统进入空闲状态，资源压力下降达到下限阀值，将减少VCPU个数来释放计算资源

 Page 60



- 在虚拟化环境下，有些虚拟机处于繁忙状态，有些虚拟机处于空闲状态，导致物理CPU资源不能有效利用，用户可以通过在线或离线调整VCPU数目，让处于繁忙状态的虚拟机获得更多的计算能力，提升物理CPU资源的利用率。

在线调整内存大小

- 虚拟机的内存有两个数值：
  - Memory：为虚拟机当前设置的内存值（即虚拟机启动后可以使用的总内存数）
  - MaxMemory：为虚拟机可调整内存上限
  - 在线调整Memory需小于等于MaxMemory值

 Page 61



- 如虚拟机的运行需要更多的内存才能满足要求的情况下，可通过调整内存大小满足虚拟机应用的要求

在线调整虚拟化网卡

- **挂载虚拟网卡**
  - 用户可以通过挂载虚拟网卡来增加虚拟机上的网卡个数
  - 挂载网卡后，不管是固定IP，还是DHCP，用户都需要手动配置新增网卡的IP
- **卸载虚拟网卡**
  - 用户可以通过卸载虚拟网卡来删除虚拟机上的某个虚拟网卡

 Page 62



- 如遇到虚拟机需要挂载多个网卡，提升网络性能的情况下，可挂载多个网卡；在网络要求下降的情况下，卸载网卡

在线挂载磁盘

- **挂载虚拟磁盘**
  - 可以通过挂载虚拟磁盘将指定路径下的磁盘挂载到虚拟机上
  - 在线挂载虚拟磁盘，则被挂载的虚拟磁盘立即生效
  - 磁盘挂载成功后，在虚拟机界面上将出现“发现新硬件，按界面提示操作后，若遇到“转换为动态磁盘”对话框，请去除复选框前的选择，再单击“确定”
- **卸载虚拟设备**
  - 可以通过卸载虚拟磁盘来删除虚拟机上的某个虚拟磁盘
  - 不允许卸载系统盘，否则虚拟机无法正常启动

 Page 63



- 如虚拟机需要的存储容量扩大的时候，可通过挂载虚拟化磁盘，加大磁盘容量，满足高容量存储需求（需存储更多的文件等）



目录

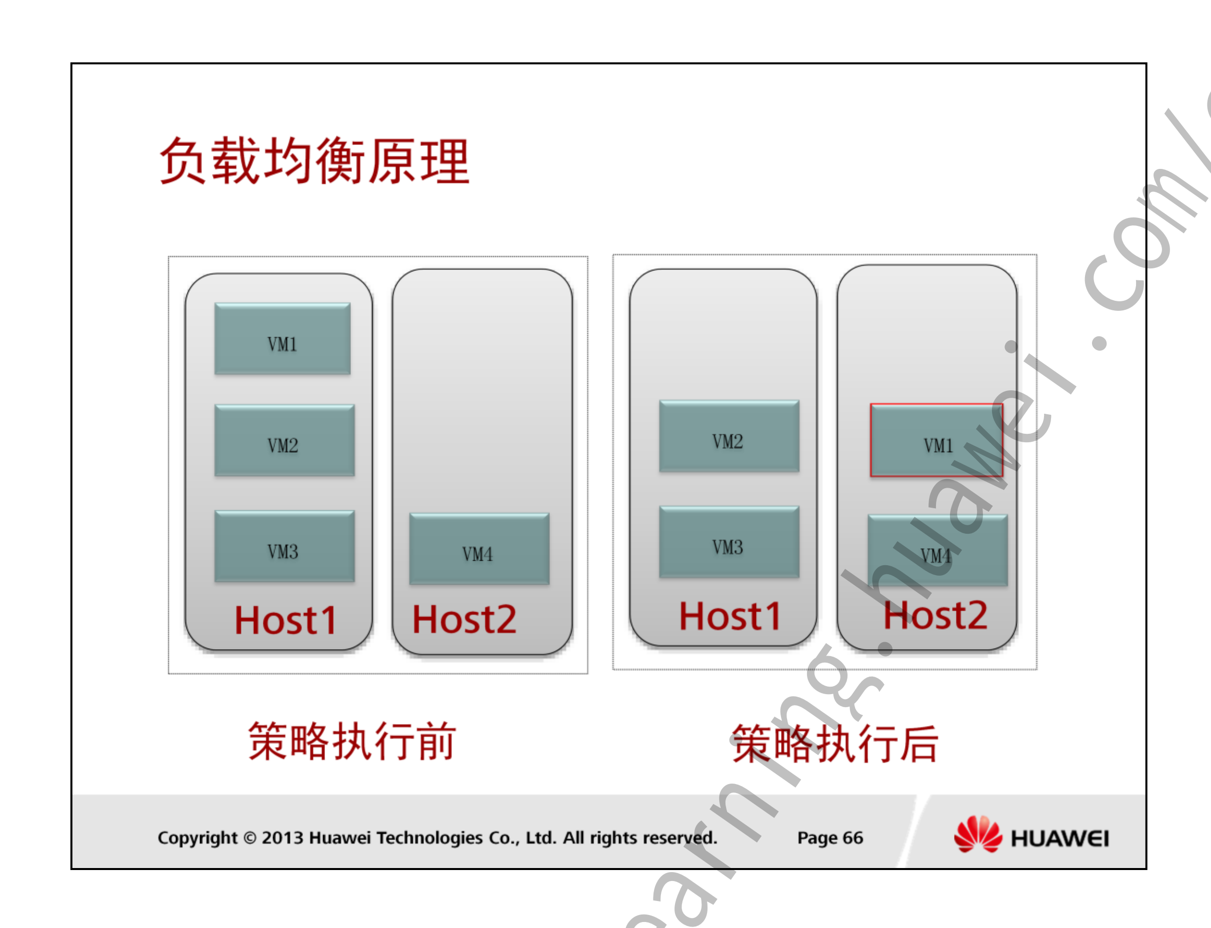


计算资源调度介绍

- 计算资源调度是什么?
  - 利用虚拟机热迁移技术自动调整虚拟机在计算节点的布局
- 计算资源调度有哪些功能?
  - 计算节点负载均衡
  - 空闲资源过多时自动下电节点；空闲资源不足时自动上电计算节点
  - 实现虚拟机间互斥、限制虚拟机运行在指定的一组主机上
- 计算资源调度可配置哪些策略?
  - 负载均衡策略
  - 电源管理策略
  - 高级调度规则

 Page 65

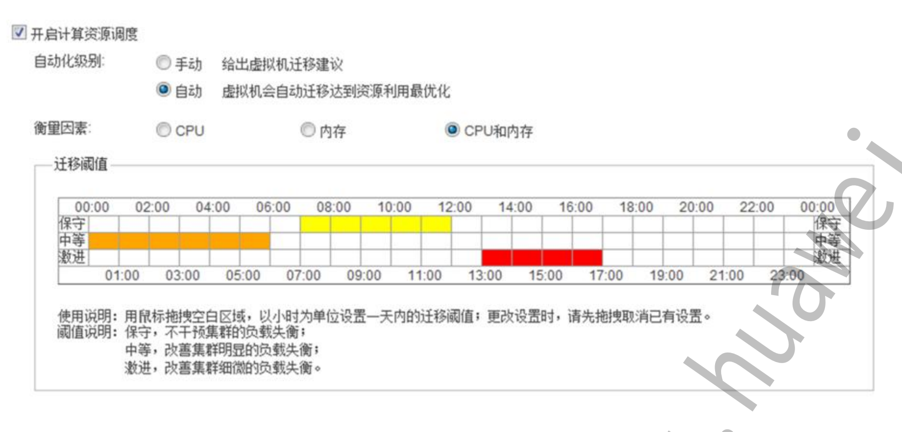




1：假设每个虚拟机的CPU、内存占用率化作计算节点的CPU、内存占用率均为10%，Host1、Host2的占用率分别为30%、10%。

2：运行负载均衡管理策略Host1上的虚拟机迁移至Host2

负载均衡策略介绍

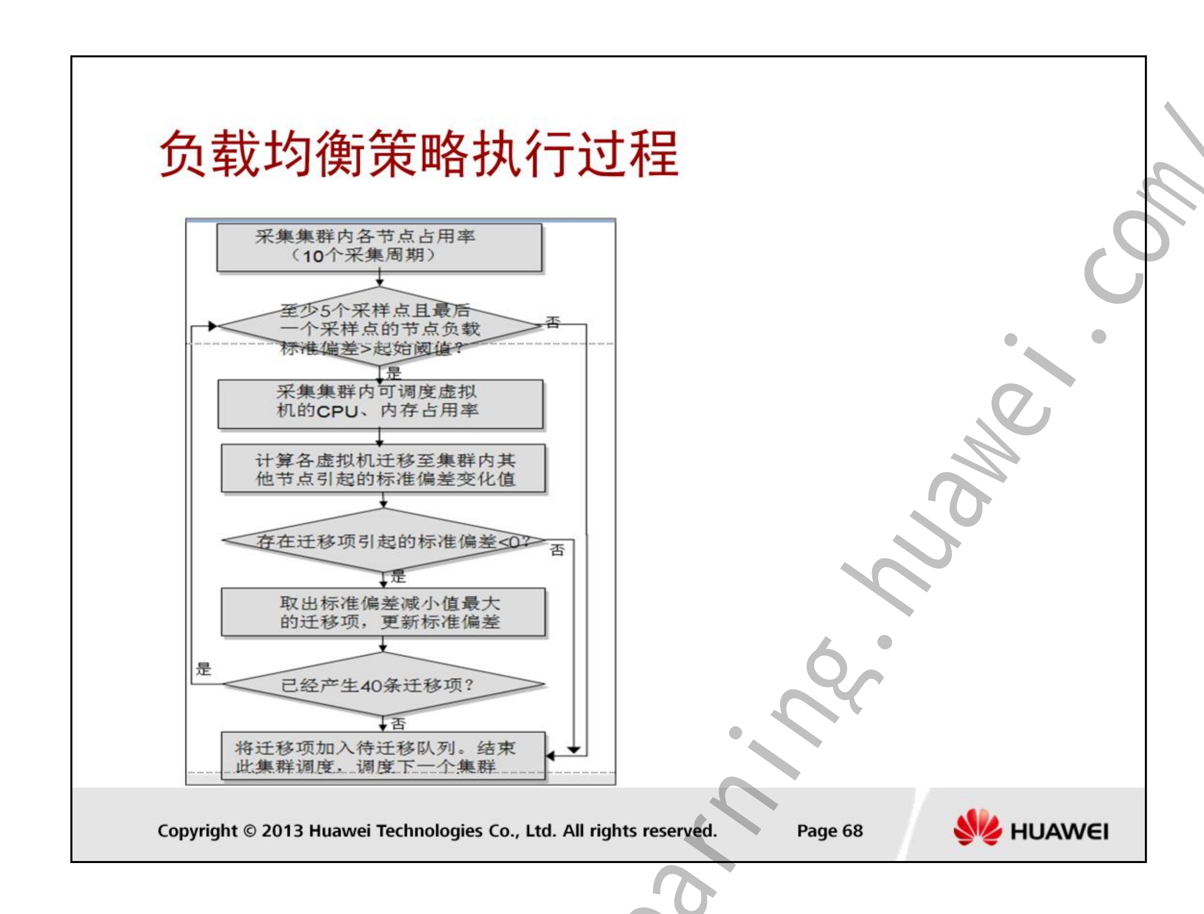


- 系统根据用户配置的策略通过热迁移虚拟机使得集群下各正常（与管理节点通信正常且未隔离）节点CPU/内存/CPU及内存占用率尽量均衡。
- 两次执行负载均衡策略的时间间隔为50min。

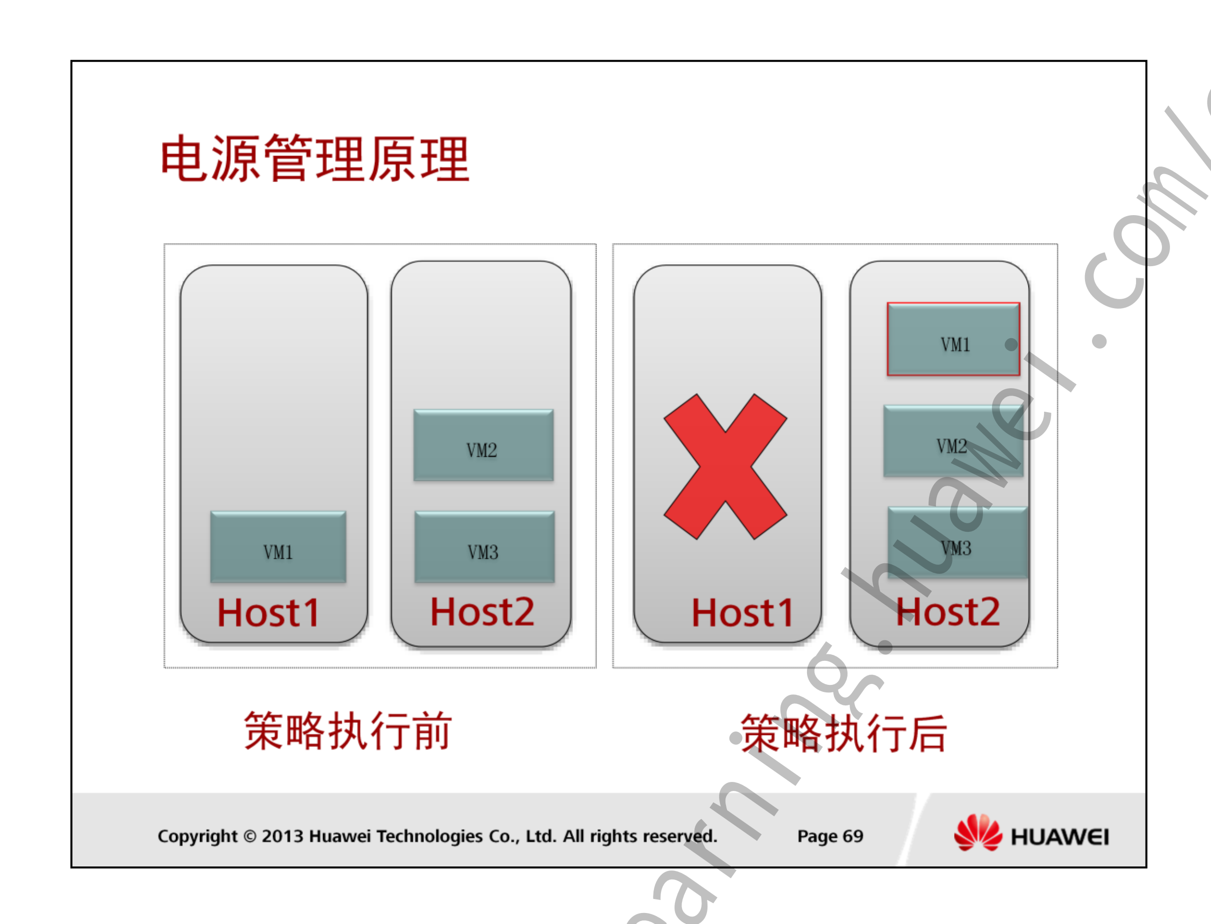
 Page 67



- 开启计算资源调度：只有打开调度开关才能设置负载均衡策略、节能减排策略、调度高级规则
- 自动化级别：分为手动和自动。
  - 手动：负载均衡时，系统给出迁移建议，管理员从portal上应用迁移建议；
  - 自动：系统自动触发虚拟机迁移，以最大可能的达到平衡。
- 衡量因素：系统根据集群下各节点的CPU占用率、内存占用率、CPU和内存占用率的差异程度决策虚拟机迁移
- 迁移阈值：表格中横轴代表时间，纵轴代表激进程度，设置粒度为小时。不同激进程度对应的颜色不同，白色表示不执行负载均衡调度
- 阈值说明：集群内主机占用率标准方差初始阈值。保守：不调度；中等：0.282；激进：0.07



- 初始阈值：中等阈值 = 初始阈值×sqrt(N)×2÷3；激进阈值 = 初始阈值×sqrt(N)×2÷12
- VM从主机A迁移至主机B，主机A的CPU/内存占用率减小：虚拟机CPU/内存占用率×虚拟机CPU/内存规格÷主机A的CPU/内存总值；主机B的CPU/内存占用率减小：虚拟机CPU/内存占用率×虚拟机CPU/内存规格÷主机B的CPU/内存总值



1：假设每个虚拟机的CPU、内存占用率化作计算节点的CPU、内存占用率均为10%，Host1、Host2的占用率分别为10%、20%。

2：运行负载均衡管理策略Host1上的虚拟机迁移至Host2，Host1进行下电。

电源管理策略介绍

提示：电源管理自动化使用BMC远程管理主机电源。请在启动电源管理自动化，针对每个主机单独配置BMC。未正确配置BMC的主机，不会自动执行电源管理。

☑ 开启电源管理自动化

电源管理阈值



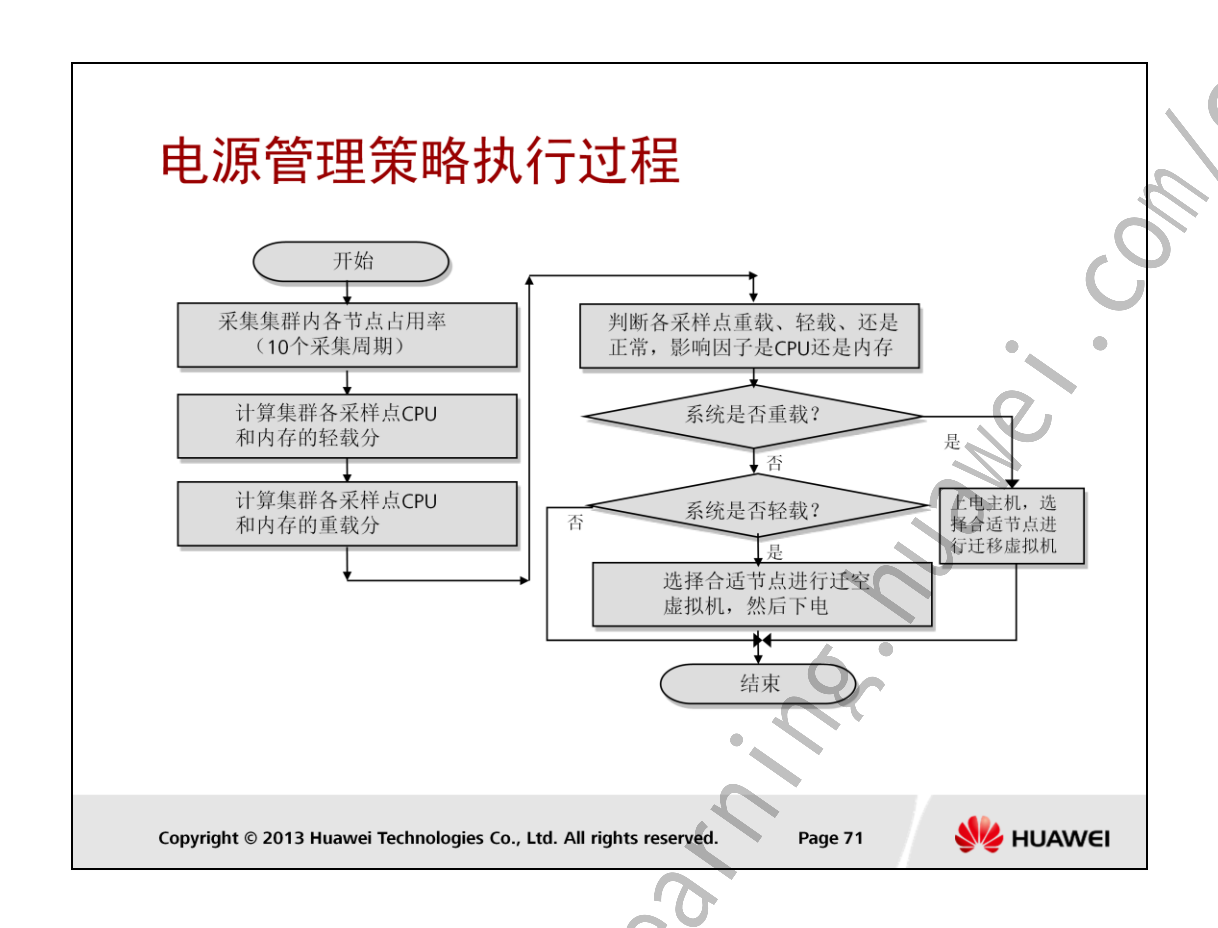
使用说明：用鼠标拖拽空白区域，以小时为单位设置一天内的迁移阈值；更改设置时，请先拖拽取消已有设置。
阈值说明：保守，如果主机资源利用率极度高于目标利用率范围，则会对主机上电；
如果主机资源利用率极度低于目标利用率范围，则会对主机下电；
中等，如果主机资源利用率明显高于目标利用率范围，则会对主机上电；
如果主机资源利用率明显低于目标利用率范围，则会对主机下电；
激进，如果主机资源利用率高于目标利用率范围，则会对主机上电；
如果主机资源利用率低于目标利用率范围，则会对主机下电；

- 系统根据用户配置的策略进行主机电源管理
- 当集群主机轻载时自动迁空主机上虚拟机并下电主机；重载时自动上电主机
- 两次执行电源管理策略时间间隔为10min

 Page 70



- 电源管理自动化开关：只有开启电源管理自动化后，管理员才可以设置各时间段的电源管理阈值
- 电源管理阈值设置中：表格中横轴代表时间，纵轴代表激进程度，设置粒度为小时。不同激进程度对应的颜色不同，白色表示不执行自动上下电；



- 轻载分计算方法：各节点的轻载值（若CPU/内存占用率小于轻载阈值则轻载值为轻载阈值-节点CPU/内存占用率，反之为0）平方和。
- 重载分计算方法：各节点的重载值（若CPU/内存占用率大于重载阈值则重载值为节点CPU/内存占用率-重载阈值，反之为0）平方和。
- 轻载或重载判断方法：（1）轻载分、重载分相等则不上电或下电；（2）轻载分大于重载分则轻载；（3）轻载分小于重在分则重载
- 下电时合适节点选择原则：（1）1小时内节点未自动下电；（2）该节点上的虚拟机均能进行热迁移；（3）主机上未连接FusionStorage存储
- 上电节点选择原则：（1）1小时内节点未自动上电；（2）优先选择大规格节点进行上电

高级调度规则介绍

- 什么是高级调度规则?
  - 资源调度开启时，对虚拟机进行特殊调度
  - 调度周期为50分钟
- 高级调度规则有哪些分类?
  - 虚拟机互斥：一组虚拟机两两运行在不同主机上
  - 虚拟机到主机：一组虚拟机运行在指定的一组主机上
- 高级调度规则与负载均衡和电源管理间关系
  - 优先级高于负载均衡
  - 优先级低于电源管理



高级调度规则配置 - 虚拟机互斥

- 进入集群->设置计算资源调度->规则管理，点击添加按钮，类型选择“互斥虚拟机”，进入如下页面创建互斥规则



Page 73



- 创建虚拟机互斥规则

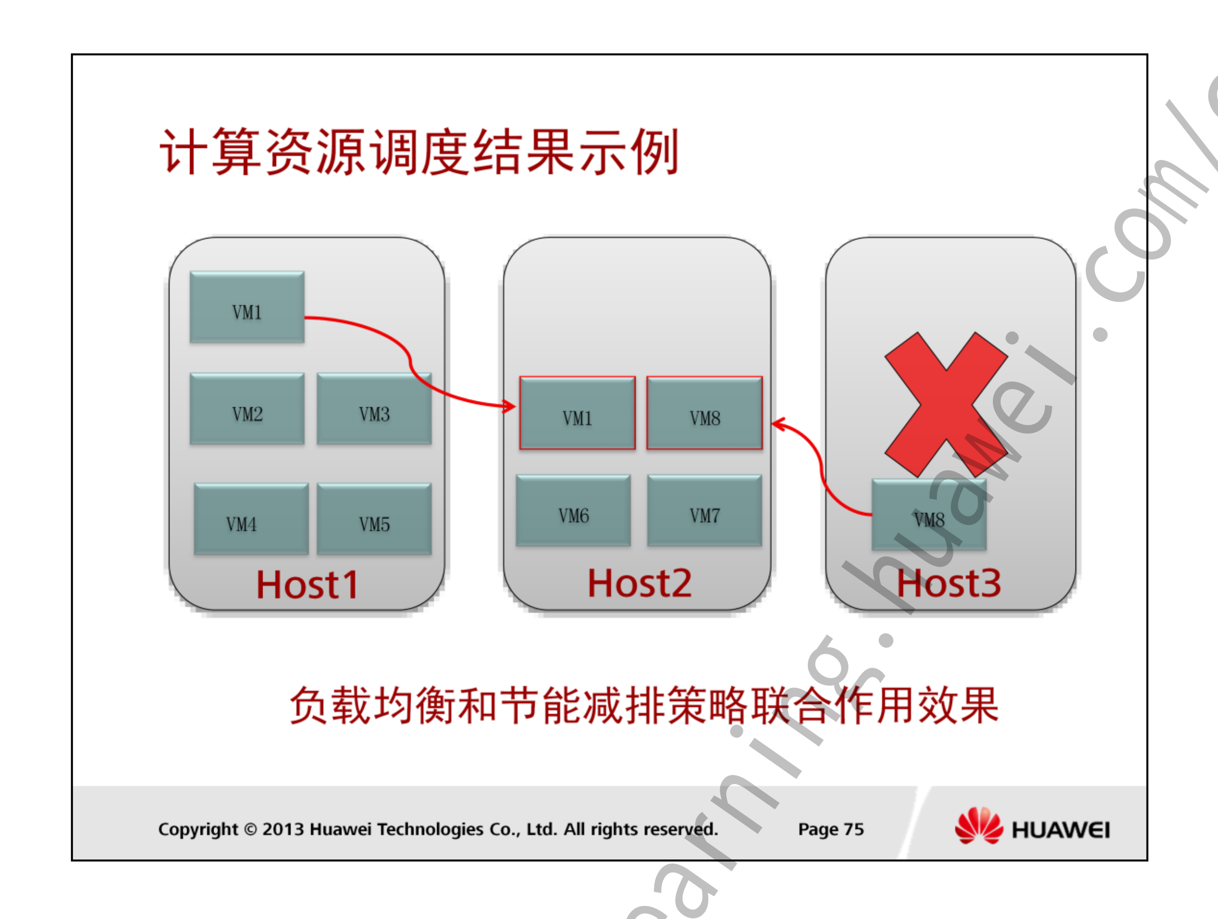
高级调度规则配置 - 虚拟机到主机

- 准备工作：创建主机组、虚拟机组
- 创建规则：进入集群->设置计算资源调度->规则管理，点击添加按钮，类型选择“虚拟机到主机”，进入如下页面创建虚拟机到主机规则





- 创建虚拟机到主机规则



0：假设每个虚拟机的cpu、内存占用率化作计算节点的CPU、内存占用率（虚拟机的CPU、内存占用率*虚拟机规格/计算节点的总资源）均为10%，Host1、Host2、Host3的占用率分别为50%、20%、10%。

1：运行电源管理策略Host3上的虚拟机迁移至Host1或Host2，然后将Host3进行下电

2：运行负载均衡使得Host1和Host2上的虚拟机均匀分布，达到均衡目的。

注：VM8最后可能位于Host1或Host2上任何一个节点上

Host2上新增的虚拟机可能为VM1~VM5、VM8中任意两个



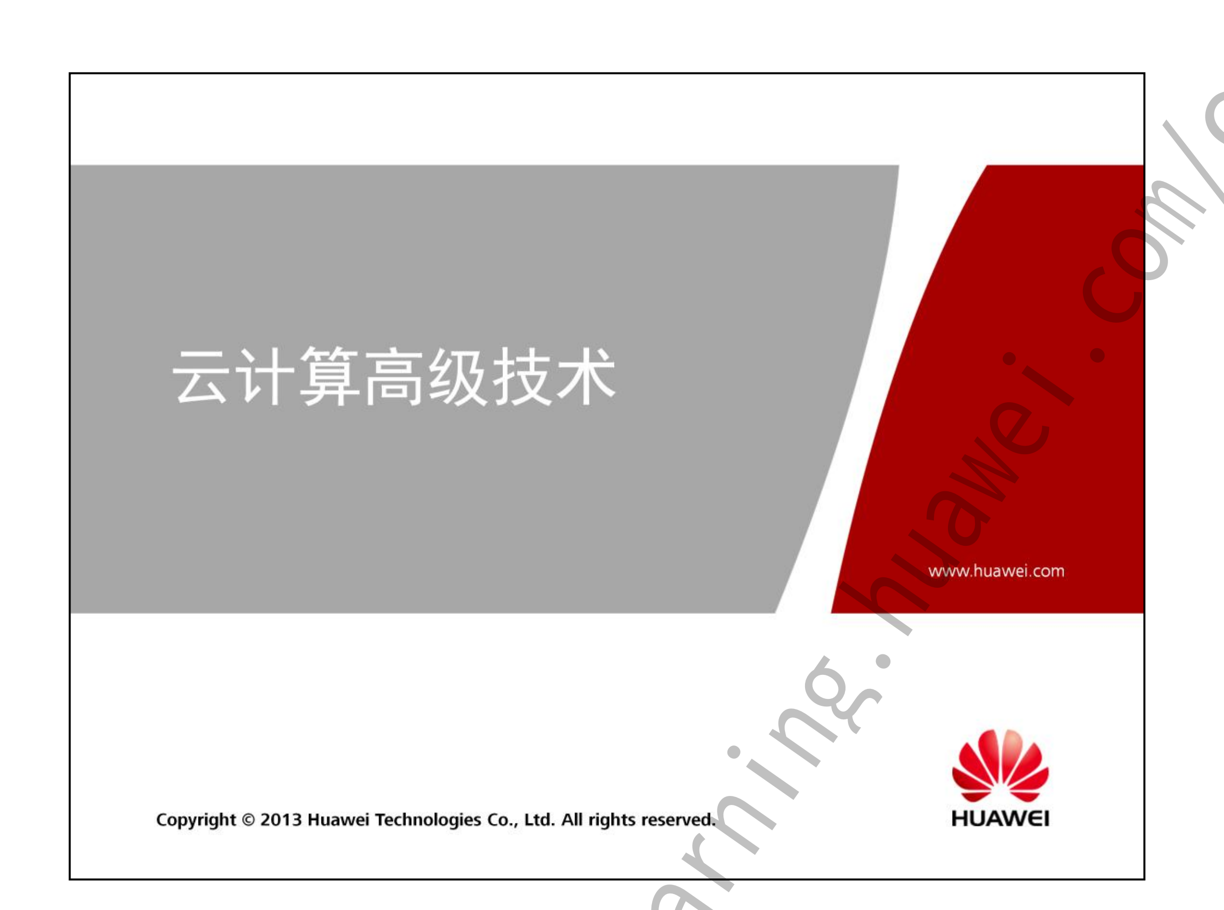
总结

- 链接克隆技术
- 内存复用技术
- 备份和恢复技术
- 虚拟机快照技术
- 虚拟机迁移技术
- 虚拟机资源在线调整技术
- 动态资源调度技术



Thank you

www.huawei.com


云计算高级技术
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

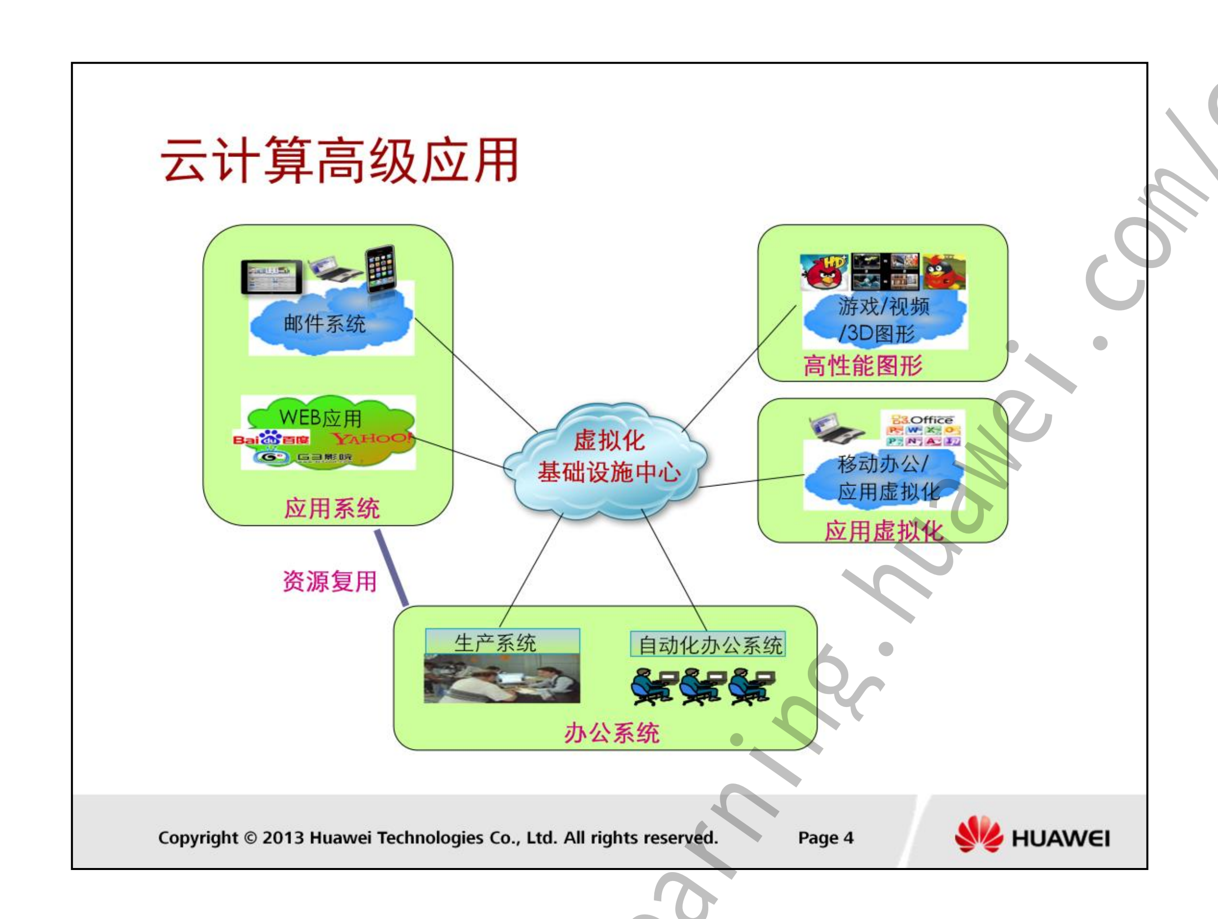
- 学完本课程后，您将能够:
  - FusionStorage的原理和应用
  - GPU直通方案的原理和应用
  - 应用虚拟化的原理和应用
  - 应用自动部署/应用弹性伸缩的原理和应用
  - 自动精简配置的应用
  - ELB原理和应用
  - VPC原理和应用





目录





云计算高级应用场景包括：

- 资源复用：不同的应用，在不同时段，分别使用虚拟化资源
- 高性能视频和图形：包括游戏、视频、2D/3D的高性能图形显示
- 应用虚拟化：通过应用虚拟化进行简单业务处理，以及通过应用虚拟机进行办公。
- 办公系统/应用系统：通过虚拟化桌面进行办公，或者支持虚拟化业务。

云计算高级技术

应用场景	高级技术
高性能图形	• GPU直通
应用虚拟化	• 应用虚拟化
资源复用	• ELB
公共	• 部署：应用自动部署、VPC、EC2 • 存储：FusionStorage存储设备、自动精简配置





目录







目录

2. FusionStorage

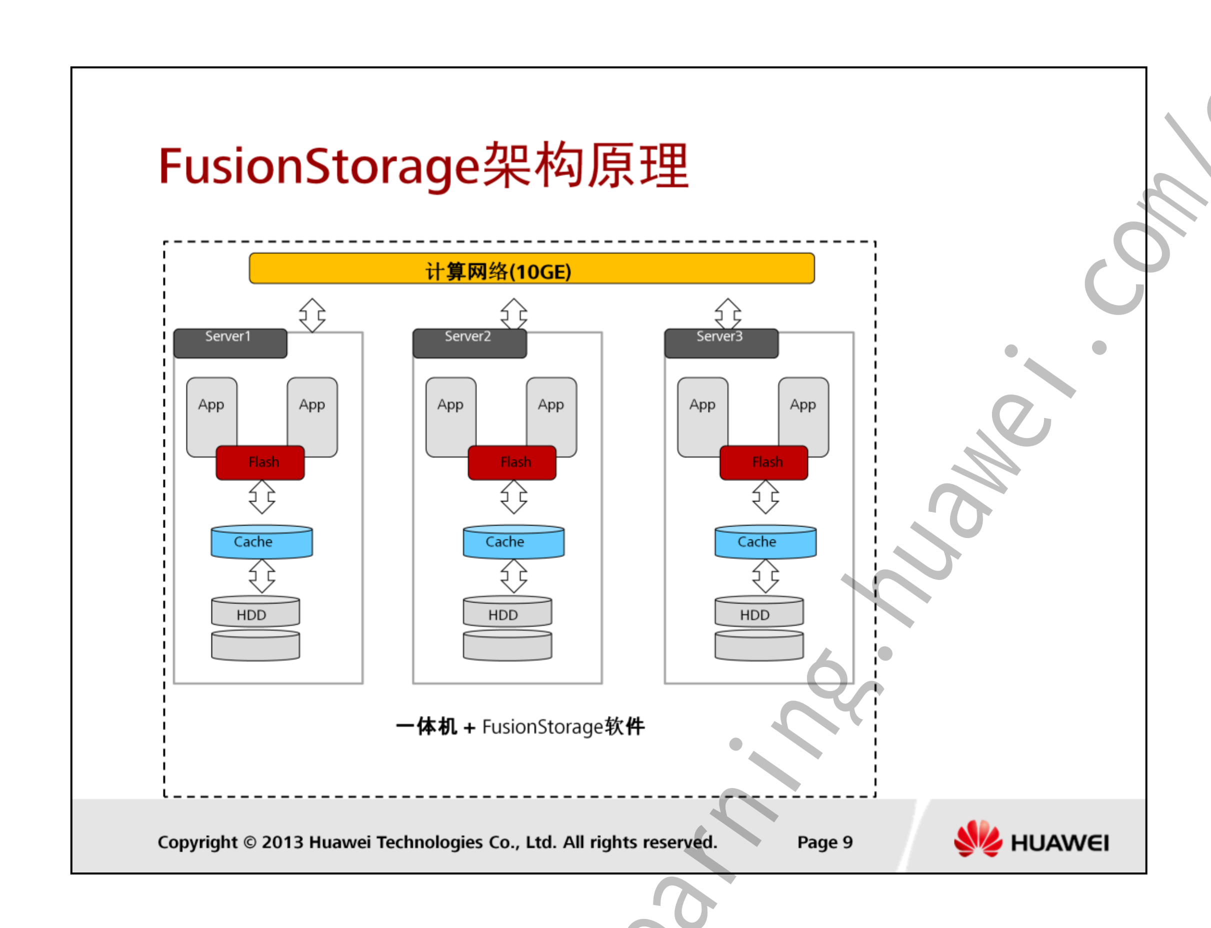


FusionStorage的诞生

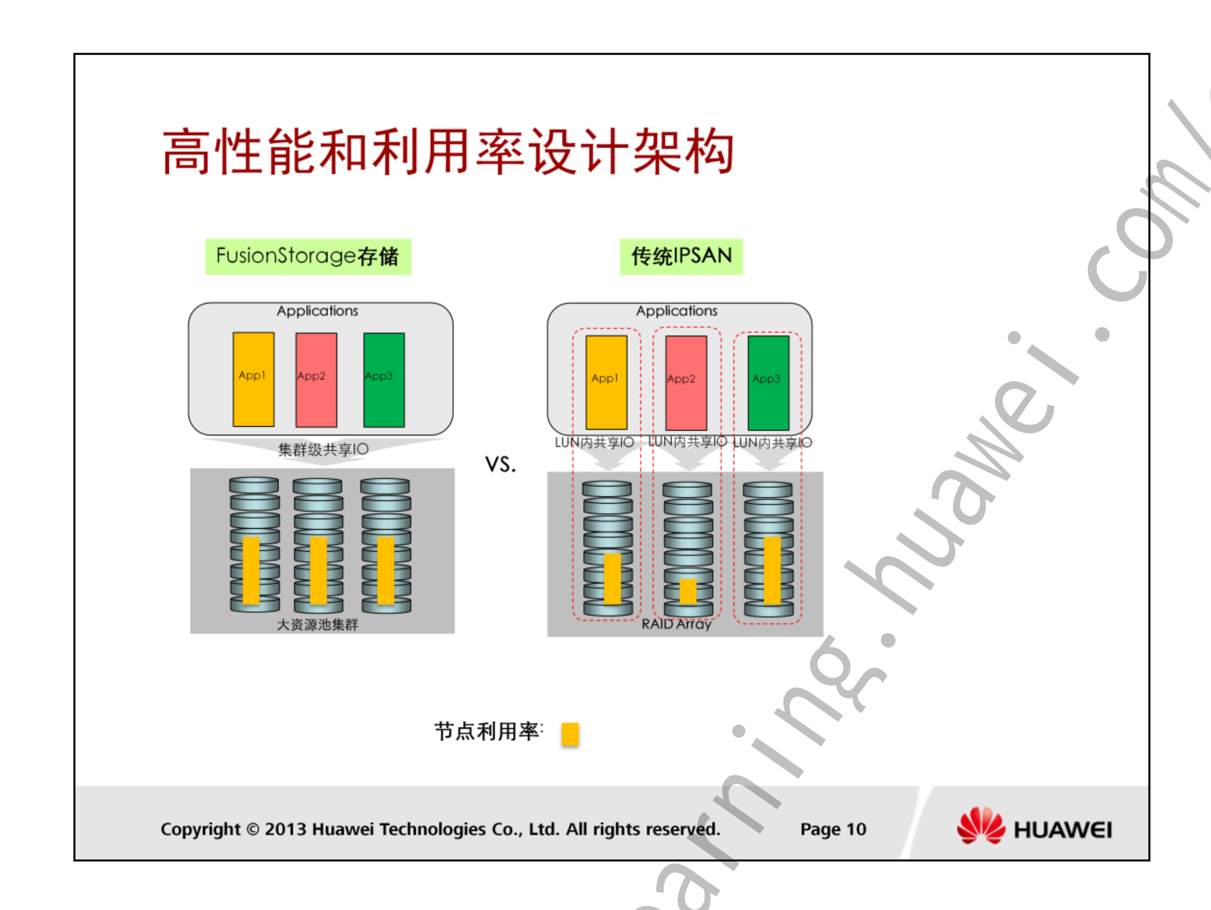
- 随着云计算、大数据等技术的兴起，对存储的性能、可靠性、可扩展性、易用性以及成本提出了更高的要求。而传统存储系统，由于架构的限制，已经无法满足企业的需求，成为阻碍企业ICT发展的瓶颈。
- 分布式存储FusionStorage是华为公司设计，完全自主产权的分布式存储架构。作为一种存储与计算高度融合的存储软件，通过突破性的架构和设计，达到高性能、高可靠、高性价比。它具有一致的、可预测的性能及可扩展性，具有高弹性和自愈能力，具有计算存储高度融合。

 Page 8





- FusionStorage是新一代分布式存储架构，它采用了大规模并行的分布式网格存储技术，使用了“横向扩展”的存储架构，利用分布式多节点网格并行分担存储负荷，并通过细粒度数据分布算法保证数据的恒定均衡分布，它不但提高了系统的可靠性、可用性和存取效率，还易于扩展。简单地说，FusionStorage总体思想是通过在通用服务器上部署该软件，可以将所有服务器的本机磁盘组织成一个虚拟存储资源池，卷被切片分割打散到整个资源池所有硬盘中，每个server节点就是一个机头控制器。



- 卷被切片分割打散到整个资源池所有硬盘中，条带化宽度增加，单卷可获得的性能大幅提升；
- 无需预先设置固定RAID组，大资源池适应应用负载的动态变化，资源池中各节点的利用率相同；
- 访问均衡，无热点，资源池中各节点的利用率相同

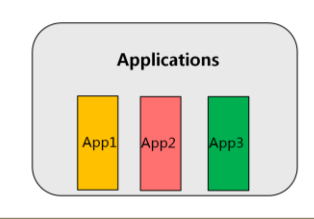


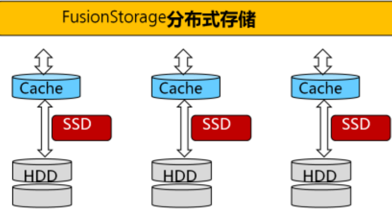
目录

2. FusionStorage



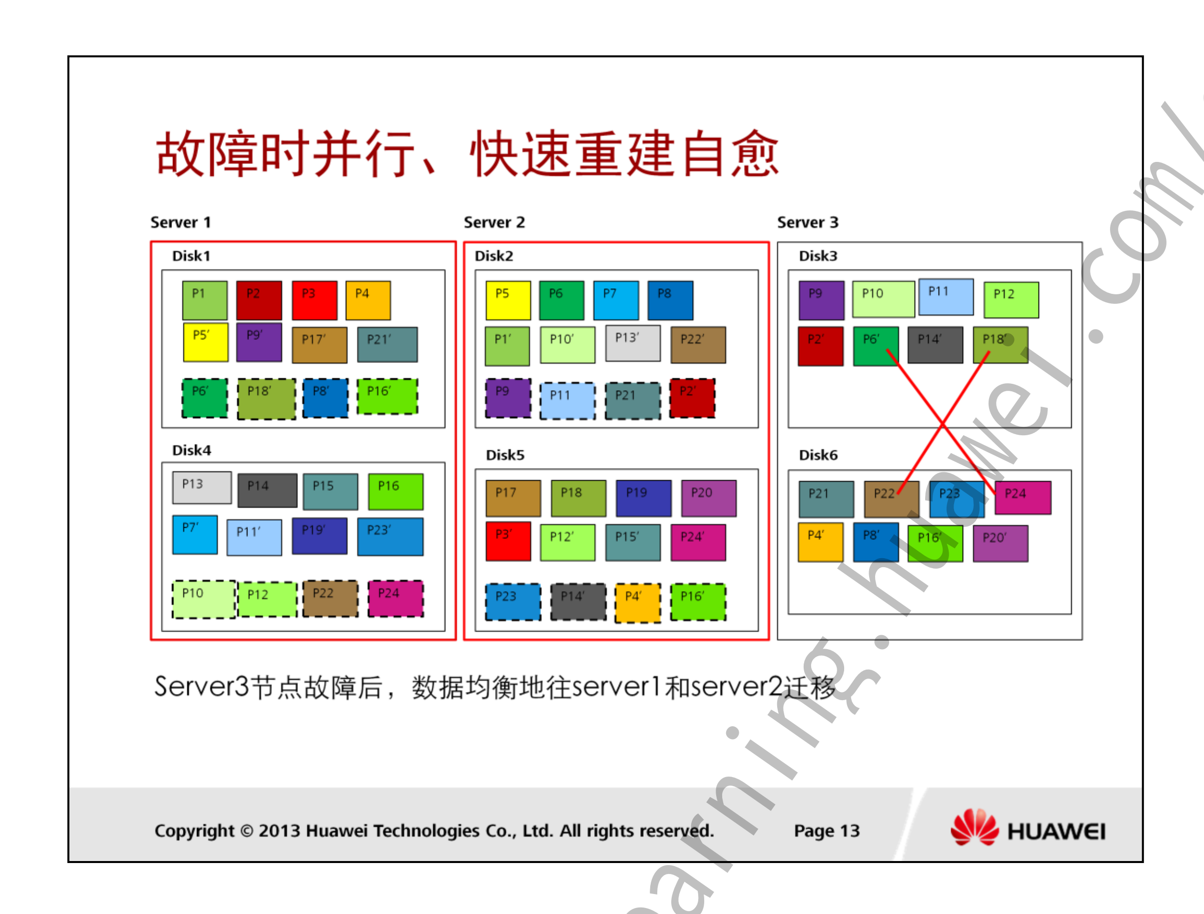
多重数据安全保障机制



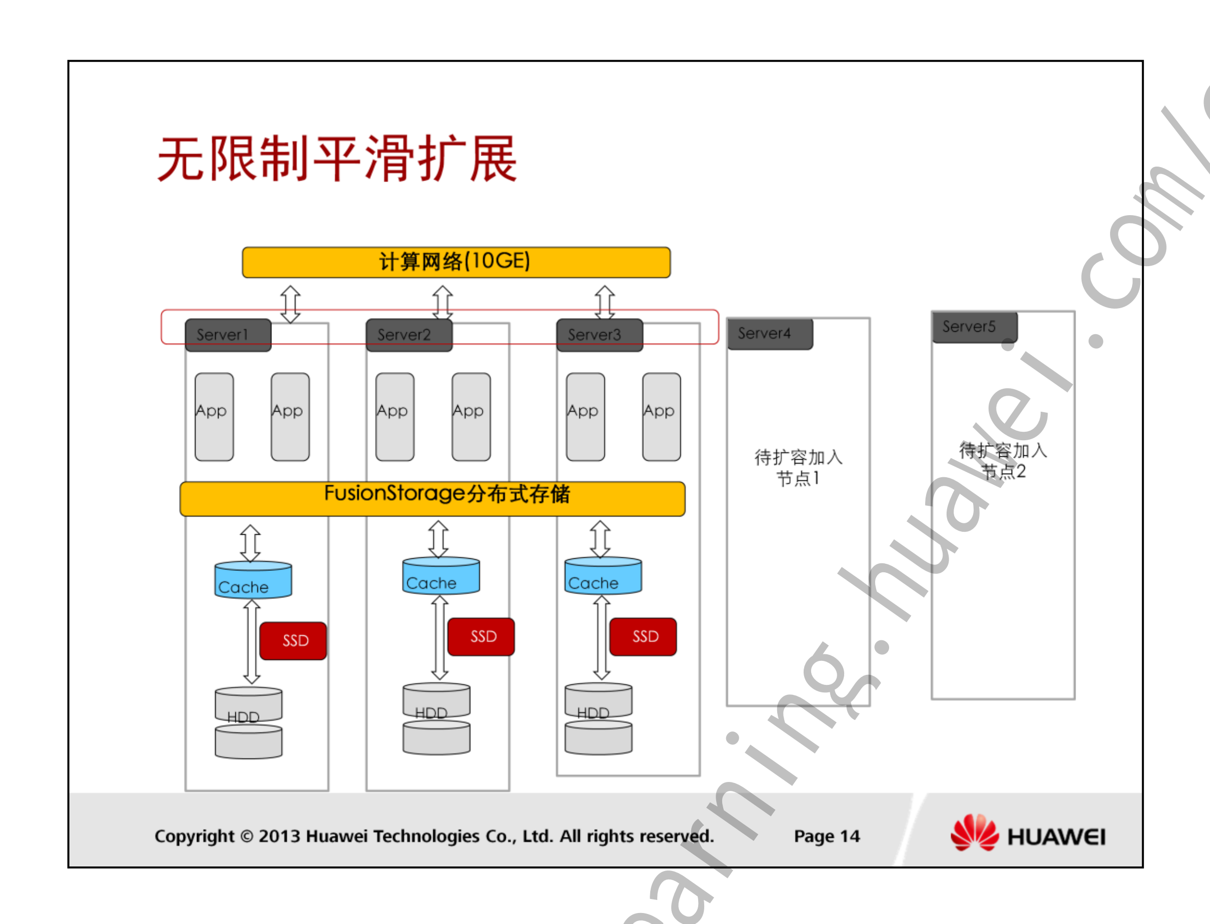


- 多副本备份：根据安全级别可灵活配置1副本（相当于RAID10）或多副本（3副本情况下，数据可用性达到11个9）
- NVDIMM Cache技术：读写速度快，掉电数据不丢失
- 强一致性复制协议：应用程序写入一份数据时，如果成功，后端的一份或多份副本必然一致，再次读时，无论从哪个副本都可读到正确的数据





- 数据分布上可以跨服务器或跨机柜，不会因某个服务器故障导致的数据不可访问；
- 数据分片在资源池内打散，硬盘故障后，可在资源池范围内自动并行重建，1TB < 30分钟（48节点），而且仅重建实际数据，无需热备盘，无需人工干预；（一般外置SAN构建1TB数据需要6~25小时）



- FusionStorage机头无状态，可横向扩展；（每server服务器一个机头）
- FusionStorage存储与计算同步平滑扩展；（非烟囱式扩展）
- 扩容后无需调整应用部署，即可获得更大的容量和性能；（系统自动负载均衡）
- 扩容时支持即插即用，扩容后系统自动调整负载平衡，真正实现无级平滑扩容

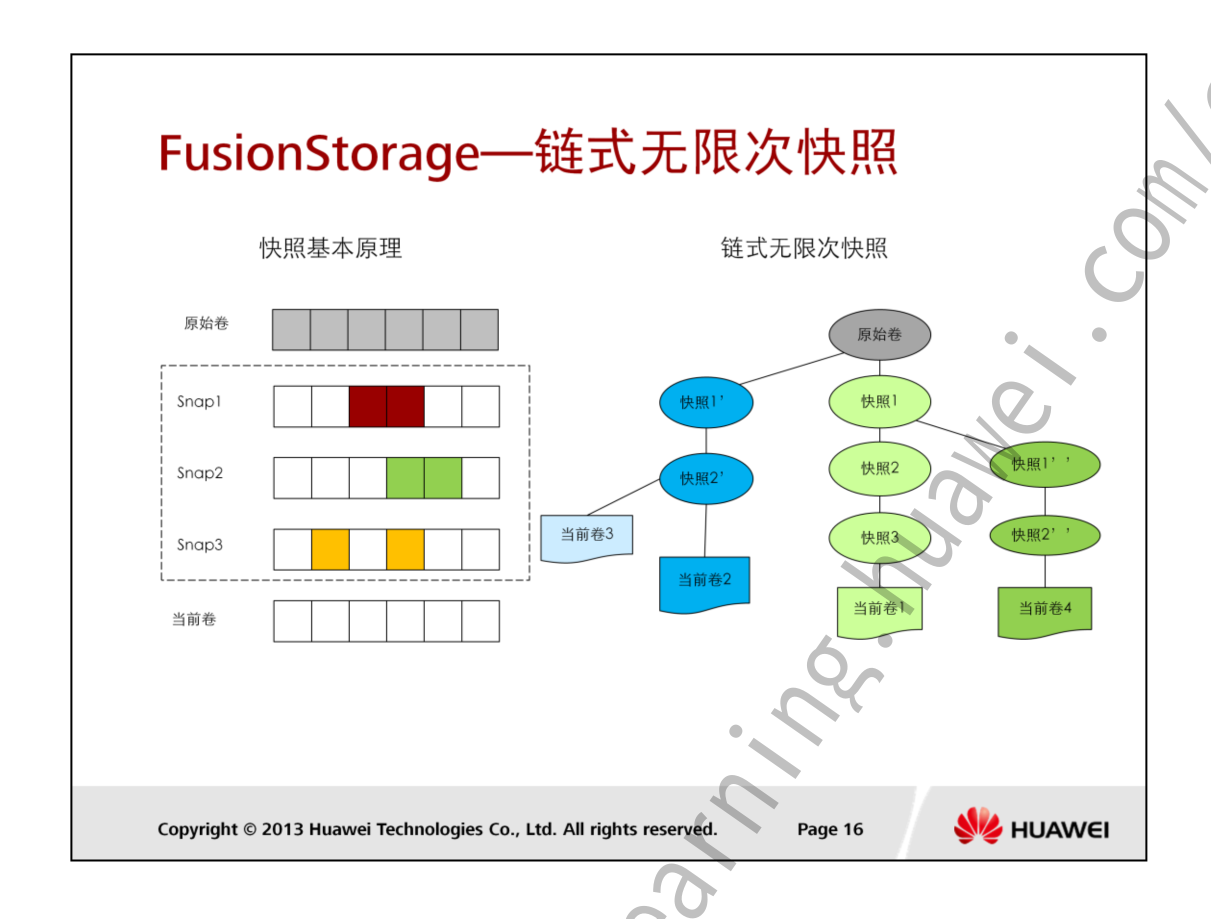
瘦分配-无任何性能下降

Volume_1　Volume_2　Volume_3　…

Disk	Disk	Disk	Disk	…	Disk	Disk
k1	k2	k3	kx		kx	kx
kx	k1	k2	k3		ky	ky
kz	kz	k1	k2		k3	kz

- 架构天然支持分布式瘦分配。
- 如图所示，当用户对卷进行写操作时才分配实际物理空间，FusionStorage仅处理虚拟卷空间和实际物理空间之间的映射关系，对性能无影响。

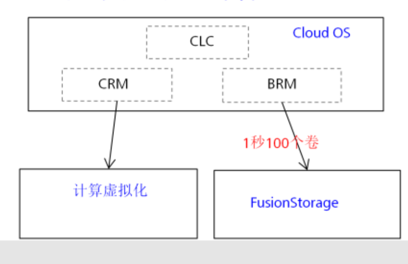




- 快照采用ROW（Redirect on write）技术，写时重定向，对卷读写性能无影响；
- 支持树状的链式快照（基于卷创快照、基于快照创卷），尤其适合于链接克隆场景，大大节省磁盘空间；(典型VDI场景下，可达1:256的链接克隆比)
- 无限次快照，不降低系统性能，同时可支持一致性快照组，用于保证对整个应用或虚拟机的一致性。

虚拟化Linked Clone和批量部署

1. Linked Clone设计原理:



主要特点:

依托FusionStorage无限次快照、性能不降低的核心技术，实现1:256的链接克隆比，构建虚拟下环境的差异化竞争力;

提升存储空间利用率;

同时提升系统性能;(将母卷通过Smart Cache机制放置在内存中)

2. 虚拟机卷批量部署:

主要特点:

支持批量进行虚拟机卷部署，能够在1秒级批量创建100个卷;

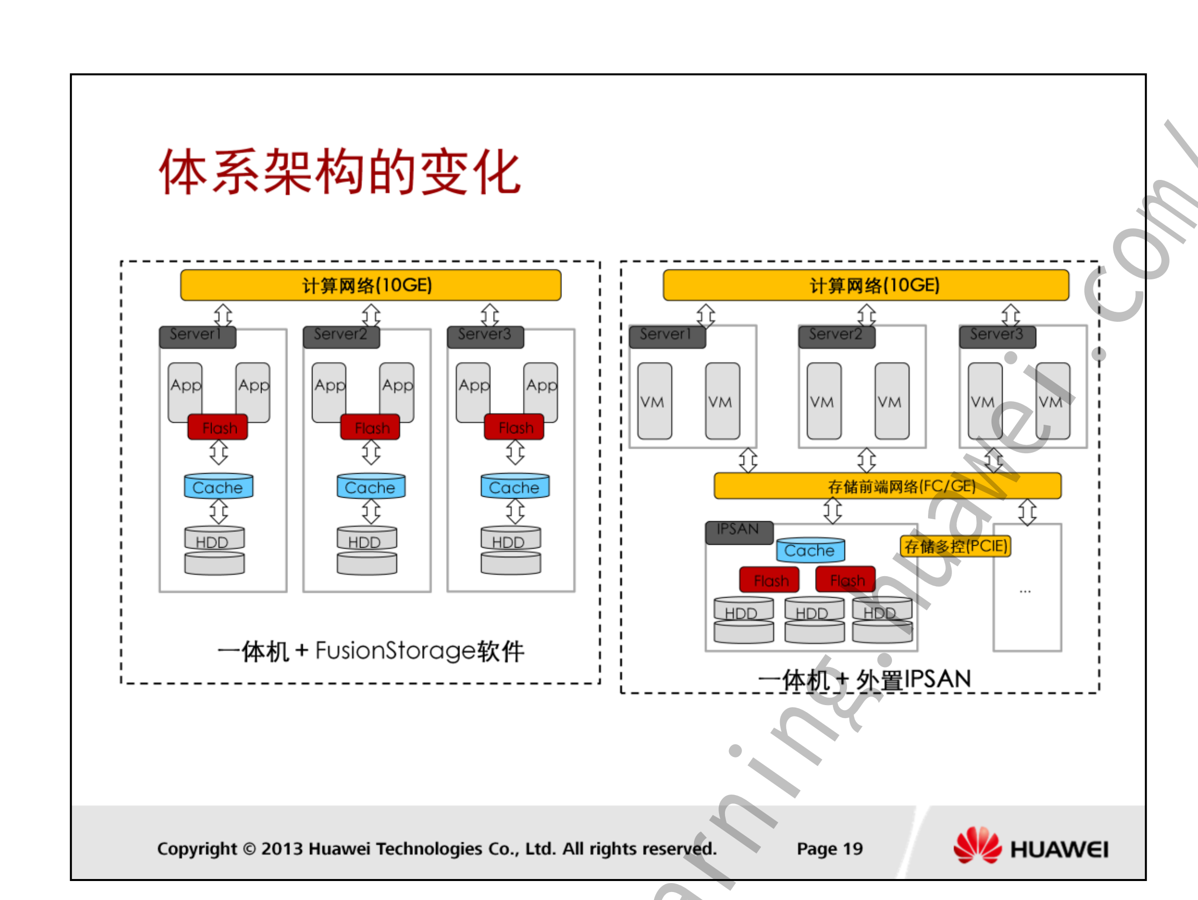




目录

2. FusionStorage




体系架构的变化
计算网络(10GE)
Server1
Server2
Server3
App
Flash
Cache
HDD
一体机 + FusionStorage软件
计算网络(10GE)
VM
存储前端网络(FC/GE)
IPSAN
存储多控(PCIE)
一体机 + 外置IPSAN
Page 19
HUAWEI

FusionStorage体系架构优势

- 扩展性
  - 机头无状态，可与计算节点同步平滑扩展；（IPSAN为烟囱式扩展）
  - 支持从3个计算刀片，平滑扩展到250个刀片的场景；满足小、中企业的需求；
- 可靠性
  - 1TB数据重建时间30分钟（48个节点规模）
  - 可跨刀片、跨机架保证可靠性；即多个机柜，故障一个机柜后，虚拟机正常运行
  - 对于一些大型高端企业需要跨站点Mirror、多点故障的场景需要高端SAN
- 性能
  - 满负荷并发性能，持平
  - 系统有余量时，应用突发性能可提升3~5倍；
  - 单应用卷性能，提升100%~300%
  - 高级功能开启下的性能不下降；（如瘦分配）
  - 对于时延极其敏感必须要PCIE、IB网络解决的高端应用，需要高端SAN



计算和存储融合体系架构优势

带宽和时延	计算存储融合	外置存储体系	备注
带宽：(盘 <--> Cache/Flash<--> 应用)	每盘100MB (本地化带宽吞吐量)	每盘20MB (后端SAS 6GB，80%利用率)	本地化的带宽吞吐，相当于将计算下移到存储侧，更好的满足如OLAP、数据分析
IO时延	本地数据：本机访问； 远端数据：1次TCP/IP交换；	本端数据：1次TCP/IP交换； 远端数据：1次TCP/IP交换，1次PCIE交换	低时延，满足高并发IOPS的需求
大容量分布式Cache	每盘1.5G~2.5G Cache	每盘0.25G Cache	SATA + 大容量Cache，达到更好的性价比



低整体拥有成本

- FusionStorage可以采用价格低廉且功耗较低SATA盘作为存储，每TB存储的价格大大降低，功耗也比传统存储节省50%。
- 一体机FusionStorage ，通过计算与存储的融合，无需外置存储，不但节省了空间，而且也免去了以往对外置存储独立供电、独立维护的成本。
- 一体机FusionStorage开局免工程配置，免存储业务配置，自动化负载均衡，故障自动化自愈，这些都大大降低了运行过程中的维护成本，管理成本。



更优的 CAPEX&OPEX

CAPEX

VDI场景性价比提升3倍

IO吞吐率相比传统 SAN存储提升30%，有效容量提升130%

中高端数据库场景 性价比提升5倍

IO吞吐率相比传统 SAN存储提升100%，有效容量提升200%

精简配置无性能损失

精简配置DSware无性能损失，外置SAN性能下降达10~20%

OPEX

无需专人维护

存储不再作为一个独立网元进行维护管理，无须专人负责存储的容量规划和配置，大大降低维护门槛

平滑扩容

支持即插即用的无级平滑扩容，相对而言，由于SAN机头的容量/处理能力限制，当容量扩展达到临界值时，需要更换机头和存储组网（如 1+1双控变为多控）

更低功耗

因使用大容量低转速SATA作为持久化存储介质，使得存储部分的系统能耗降低50%以上




HUAWEI

FusionStorage技术规格

指标名称	指标规格	备注
可支持的最大硬盘数	2000 最小规模3个服务器	可支持SAS/NL-SAS/SATA
可支持的最大逻辑卷数量	65000	卷数目增多，性能不变
单资源池最小/大规模	12~180块硬盘（2份拷贝） 12~2000块硬盘(3份拷贝)	
单卷最大快照数量	65000	快照空间没有限制
单卷支持的容量	16TB	
链接克隆比	256	性能不下降
每T数据恢复性能	<30min	VDI正常业务下，48节点以上
存储设备最大时延控制	<150ms	
支持最多的刀片数(或主机数)	250	

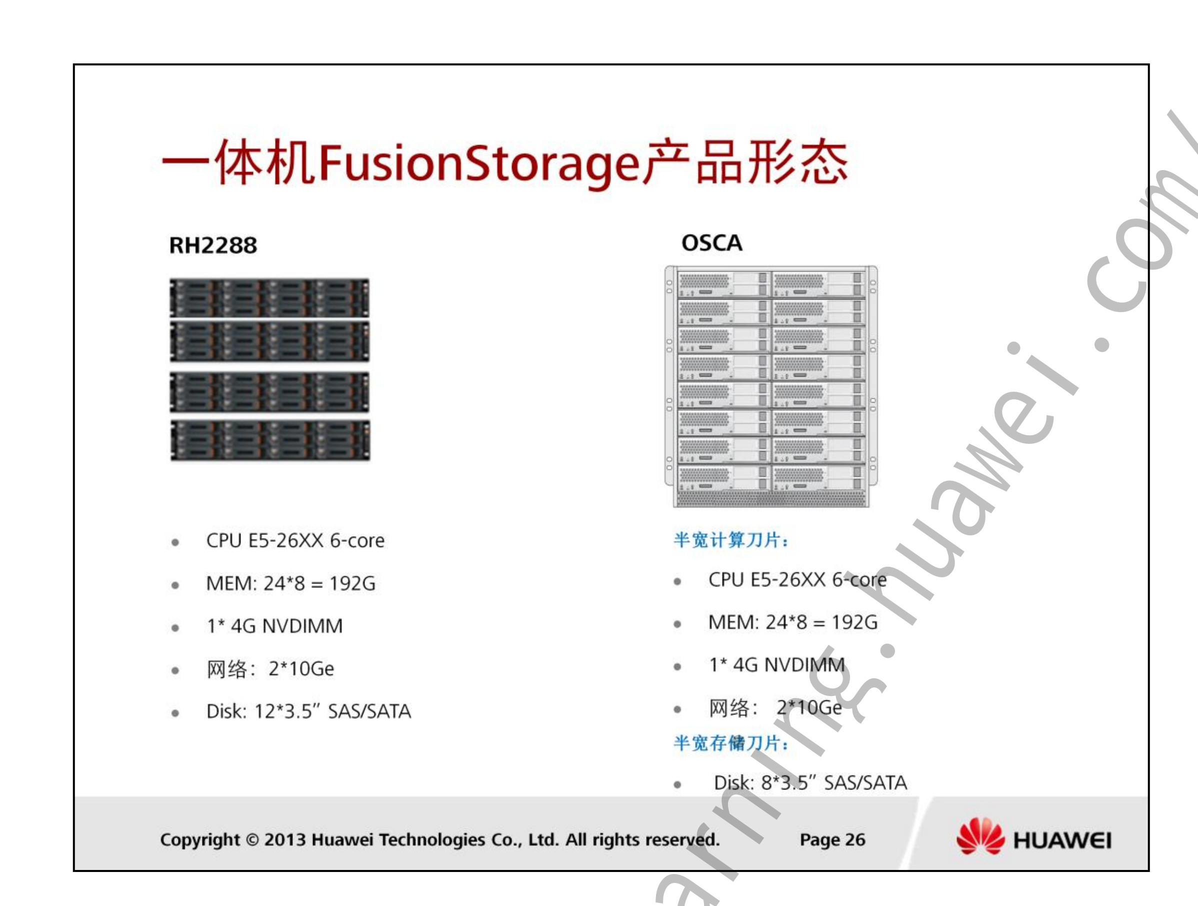




目录

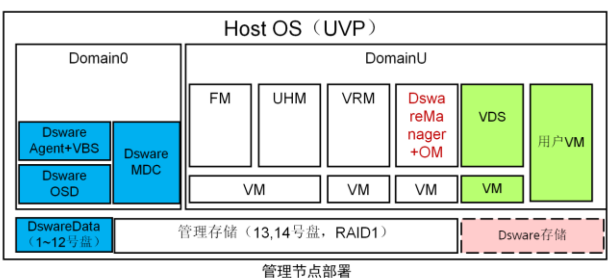
2. FusionStorage



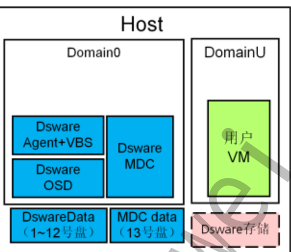


- FusionStorage将服务器本地的硬盘组织成一个虚拟化的存储资源池，对虚拟机提供网络RAID保护的卷设备

基于RH2288的部署



管理节点部署



计算节点部署

- 方案说明：
  - CNA OS安装在U盘
  - 管理节点VM使用本地存储
  - FusionStorage用于VDS、ESC、用户VM部署
- 方案特点：
  - MDC与管理节点共享本地存储；
  - 扩容存储可以最大使用12块硬盘
- 优缺点：
  - 较方案1存储密度高

MDC跟管理节点共硬盘

RH2288（2*CPU+12*3.5″ HDD） 计算节点：Dsware Agent/VBS/OSD（其中1~12号盘：Dsware数据盘）
RH2288（2*CPU+12*3.5″ HDD+1*2.5″ HDD） 计算节点：Dsware Agent/VBS/OSD/MDC（其中1~12号盘：Dsware数据盘，13号盘：MDC
RH2288（2*CPU+12*3.5″ HDD+2*2.5″ HDD） 管理节点：GM/UHM/VRM/DSware-OM/Dsware Agent/VBS/OSD/MDC（其中1~12号盘：Dsware数据盘，13/14号盘(后面)：管理节点/MDC
RH2288（2*CPU+12*3.5″ HDD+2*2.5″ HDD） 管理节点：GM/UHM/VRM/DSware-OM/Dsware Agent/VBS/OSD/MDC（其中1~12号盘：Dsware数据盘，13/14号盘(后面)：管理节点/MDC



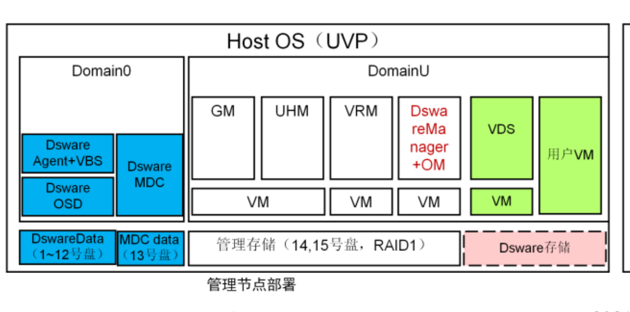
OSCA半宽单高2P计算刀片+ARM存储刀片

- 方案说明：
  - CNA OS安装在U盘
  - 管理节点VM使用本地存储
  - FusionStorage用于VDS、ESC、用户VM部署
- 方案特点：
  - MDC与管理节点共享本地存储；
- 优缺点：
  - 初始配置较方案1节点少，稍优

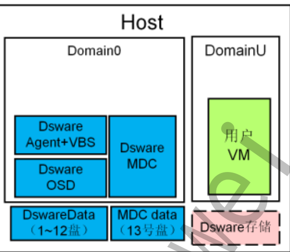
MDC跟管理节点共硬盘

半宽全高2P计算刀片（2*CPU） 计算节点:Dsware Agent/VBS	ARM存储刀片（2*ARM+8*3.5"HDD） 存储节点：Dsware Agent/OSD
ARM存储刀片（2*ARM+8*3.5"HDD） 存储节点： DswareAgent/OMAgent/OSD	ARM存储刀片（2*ARM+8*3.5"HDD） 存储节点： DswareAgent/OMAgent/OSD
半宽全高2P计算刀片（2*CPU+1*2.5" HDD) 计算节点:Dsware Agent/VBS/MDC	ARM存储刀片（2*ARM+8*3.5"HDD） 存储节点：Dsware Agent/OSD
半宽全高2P计算刀片（2*CPU+2*2.5" HDD) 管理节点：GM/UHM/VRM/DSware-OM/Dsware Agent/VBS/MDC	半宽全高2P计算刀片（2*CPU+2*2.5" HDD) 管理节点：GM/UHM/VRM/DSware-OM/Dsware Agent/VBS/MDC

OSCA全宽单高2P计算存储刀片



管理节点部署



计算节点1部署

Host
Domain0
Domain U
Dsware Agent+VBS
Dsware OSD
用户VM
DswareData（1~12盘）
Dsware存储

计算节点T2部署

方案说明：

- CNA OS安装在U盘
- 管理节点VM使用本地存储
- FusionStorage用于VDS、ESC、用户VM部署

方案特点：

- MDC独占一个磁盘，由于FusionStorage最大支持单节点12块盘配置，全宽15个盘位下，影响不大

优缺点：

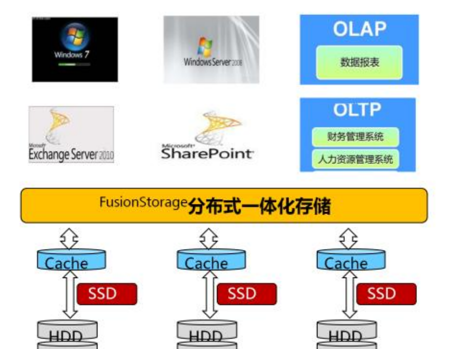
- 起步配置节点少
- MDC独占硬盘，可靠性、性能较好
- 每个管理节点较方案一多使用一块硬盘

OSCA全宽单高2P计算存储刀片（15*2.5"HDD)

OSCA全宽单高2P计算存储刀片（15*2.5"HDD)
全宽单高2P计算存储刀片（2*CPU+12*2.5 “HDD) 其它计算节点T2：Dsware Agent/VBS/OSD（其中1~12号盘：Dsware数据盘）
全宽单高2P计算存储刀片（2*CPU+13*2.5"HDD) 计算节点T1：Dsware Agent/VBS/OSD/MDC（其中1~12号盘：Dsware数据盘，13号盘：MDC）
全宽单高2P计算存储刀片（2*CPU+15*2.5"HDD) 管理节点：GM/UHM/VRM/DSware-OM/Dsware Agent/VBS/OSD/MDC（其中1~12号盘：Dsware数据盘，13号盘：MDC，14/15号盘：管理节点
全宽单高2P计算存储刀片（2*CPU+15*2.5"HDD) 管理节点：GM/UHM/VRM/DSware-OM/Dsware Agent/VBS/OSD/MDC（其中1~12号盘：Dsware数据盘，13号盘：MDC，14/15号盘：管理节点



FusionStorage适用的场景



- VDI、Exchange/SharePoint
  - 典型特点：池化容量共享瘦分配、性能共享分时复用、计算和存储配比相对均衡；成本性价比要求高；
- 虚拟化环境混合应用：
  - 典型特点：大资源池化共享需求明显，多应用混合workload；线性扩展；
- OLAP应用、大数据分析
  - 典型特点：大并发吞吐量，计算和存储带宽要求高；
- OLTP应用
  - 典型特点：IOPS并发度高

HUAWEI



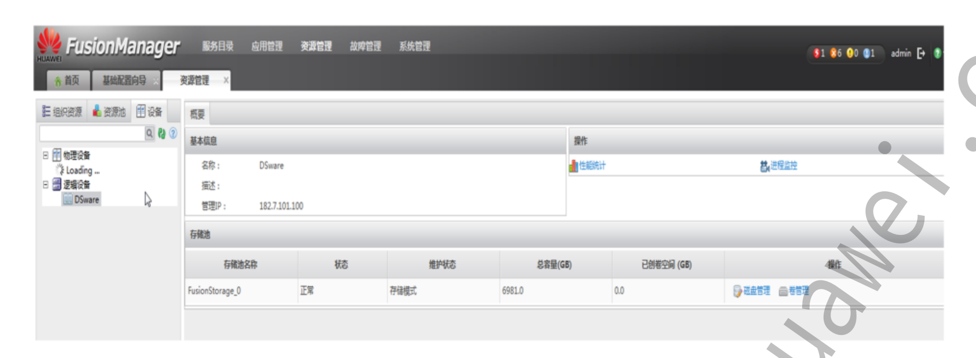




目录

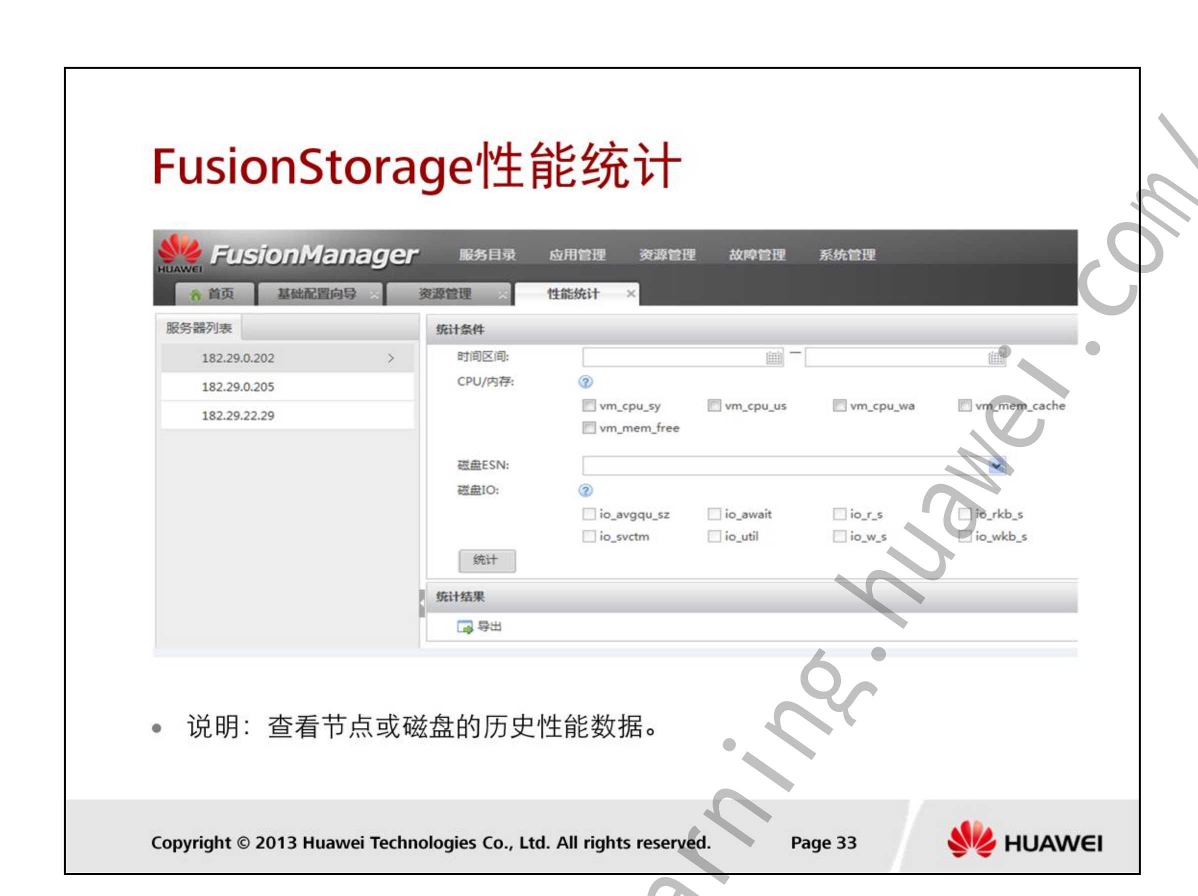


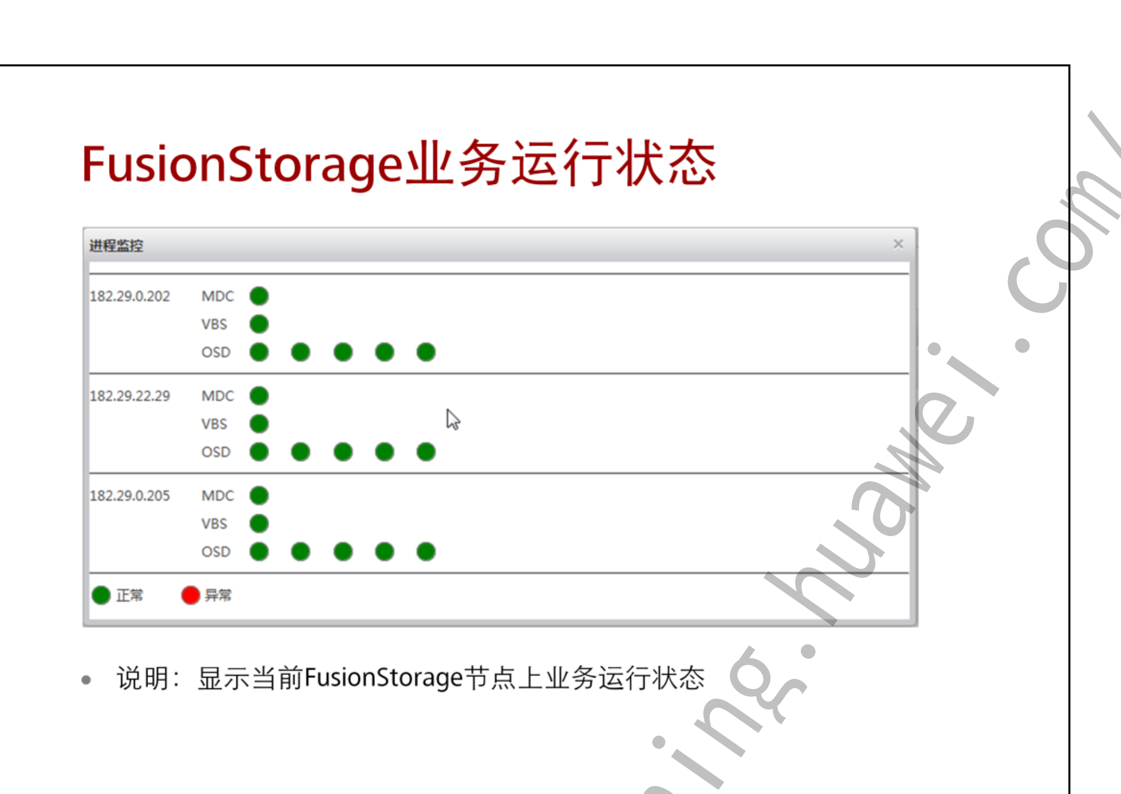
FusionStorage集群信息

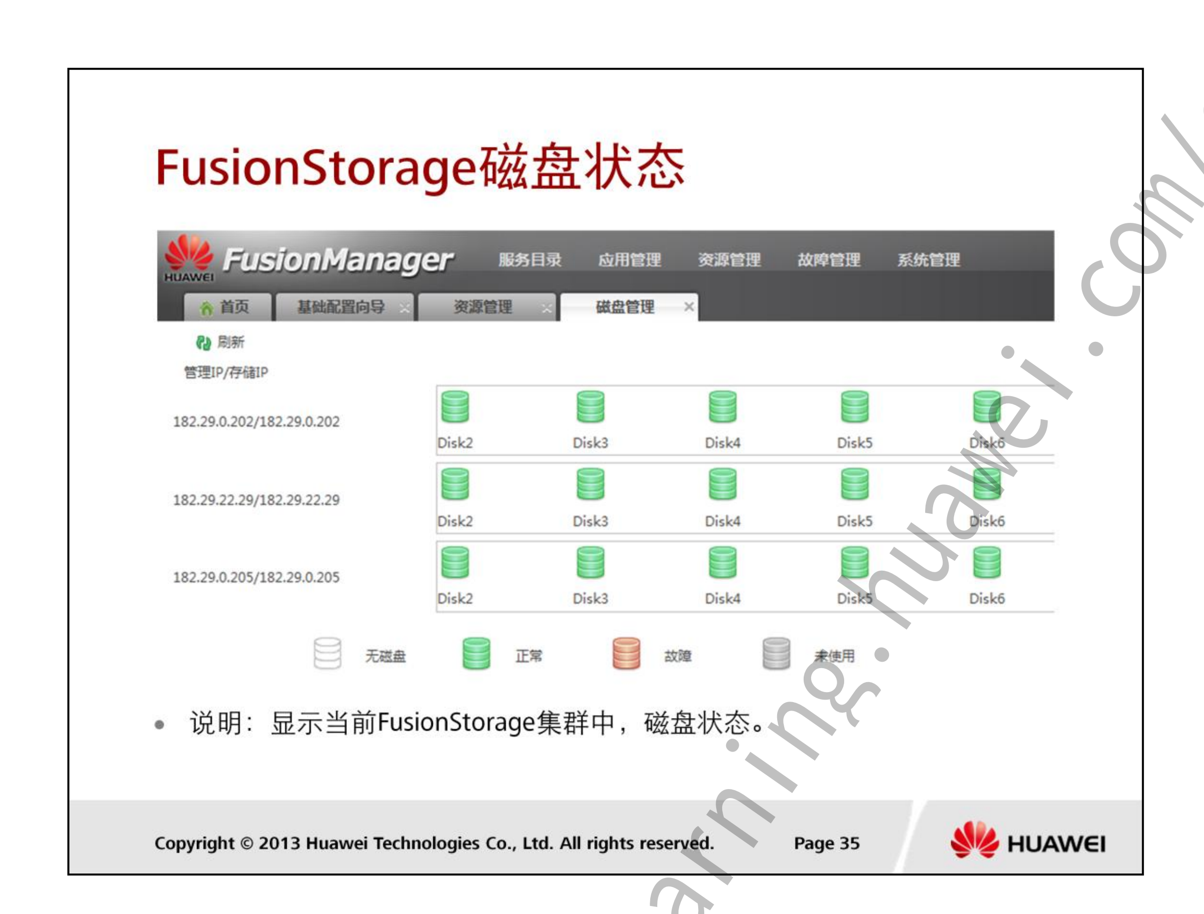


- 说明：显示FusionStorage集群整体信息，如状态，存储模式，总容量，已分配容量等信息。

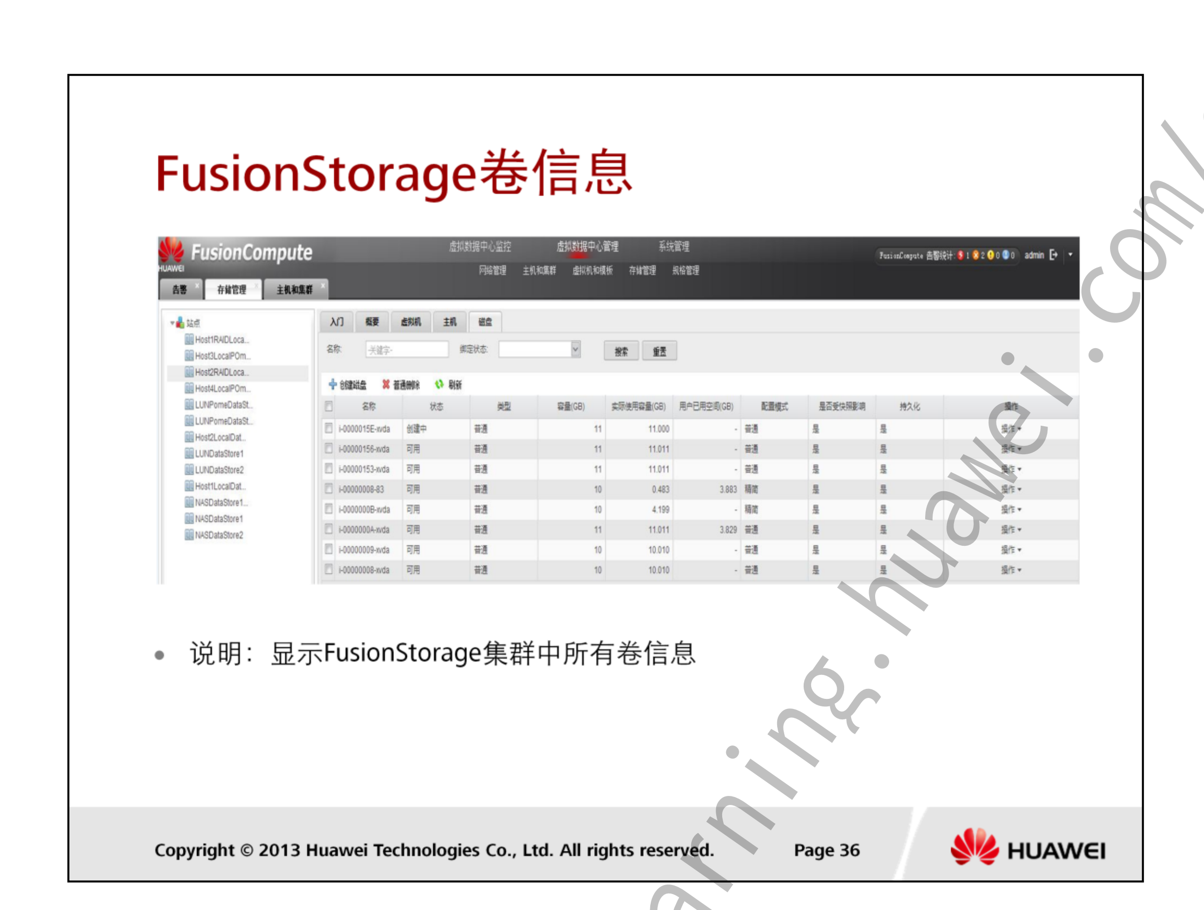



FusionStorage性能统计
FusionManager
服务目录
应用管理
资源管理
故障管理
系统管理
首页
基础配置向导
资源管理
性能统计
服务器列表
182.29.0.202
182.29.0.205
182.29.22.29
统计条件
时间区间:
CPU/内存:
vm_cpu_sy
vm_cpu_us
vm_cpu_wa
vm_mem_cache
vm_mem_free
磁盘ESN:
磁盘IO:
io_avgqu_sz
io_await
io_r_s
io_rkb_s
io_svctm
io_util
io_w_s
io_wkb_s
统计
统计结果
导出
说明：查看节点或磁盘的历史性能数据。
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 33
HUAWEI


FusionStorage业务运行状态
进程监控
182.29.0.202
MDC
VBS
OSD
182.29.22.29
MDC
VBS
OSD
182.29.0.205
MDC
VBS
OSD
正常
异常
• 说明：显示当前FusionStorage节点上业务运行状态
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 34
HUAWEI


FusionStorage磁盘状态
FusionManager
服务目录
应用管理
资源管理
故障管理
系统管理
首页
基础配置向导
资源管理
磁盘管理
刷新
管理IP/存储IP
182.29.0.202/182.29.0.202
182.29.22.29/182.29.22.29
182.29.0.205/182.29.0.205
Disk2
Disk3
Disk4
Disk5
Disk6
无磁盘
正常
故障
未使用
说明：显示当前FusionStorage集群中，磁盘状态。
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 35
HUAWEI

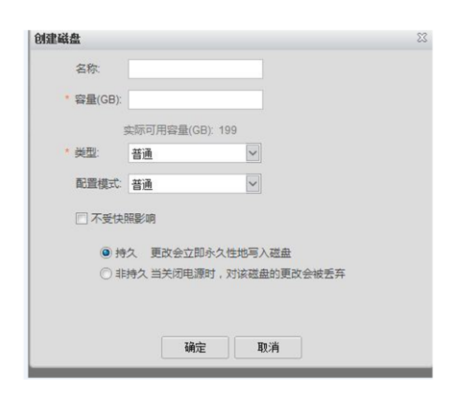
FusionStorage卷信息



- 说明：显示FusionStorage集群中所有卷信息

HUAWEI

FusionStorage操作







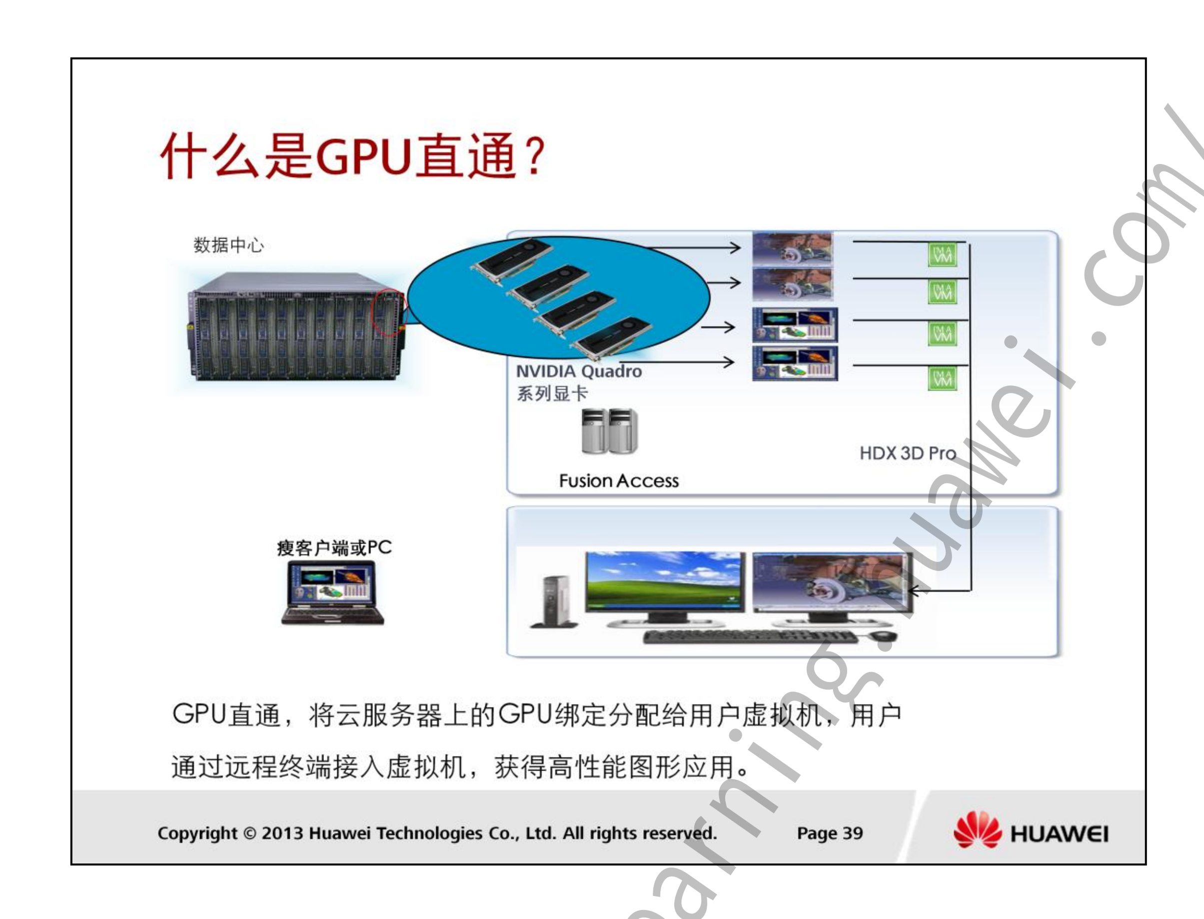
- 说明： FusionStorage提供的操作：创建卷，删除卷，创建快照，删除快照，根据快照创建卷等

HUAWEI

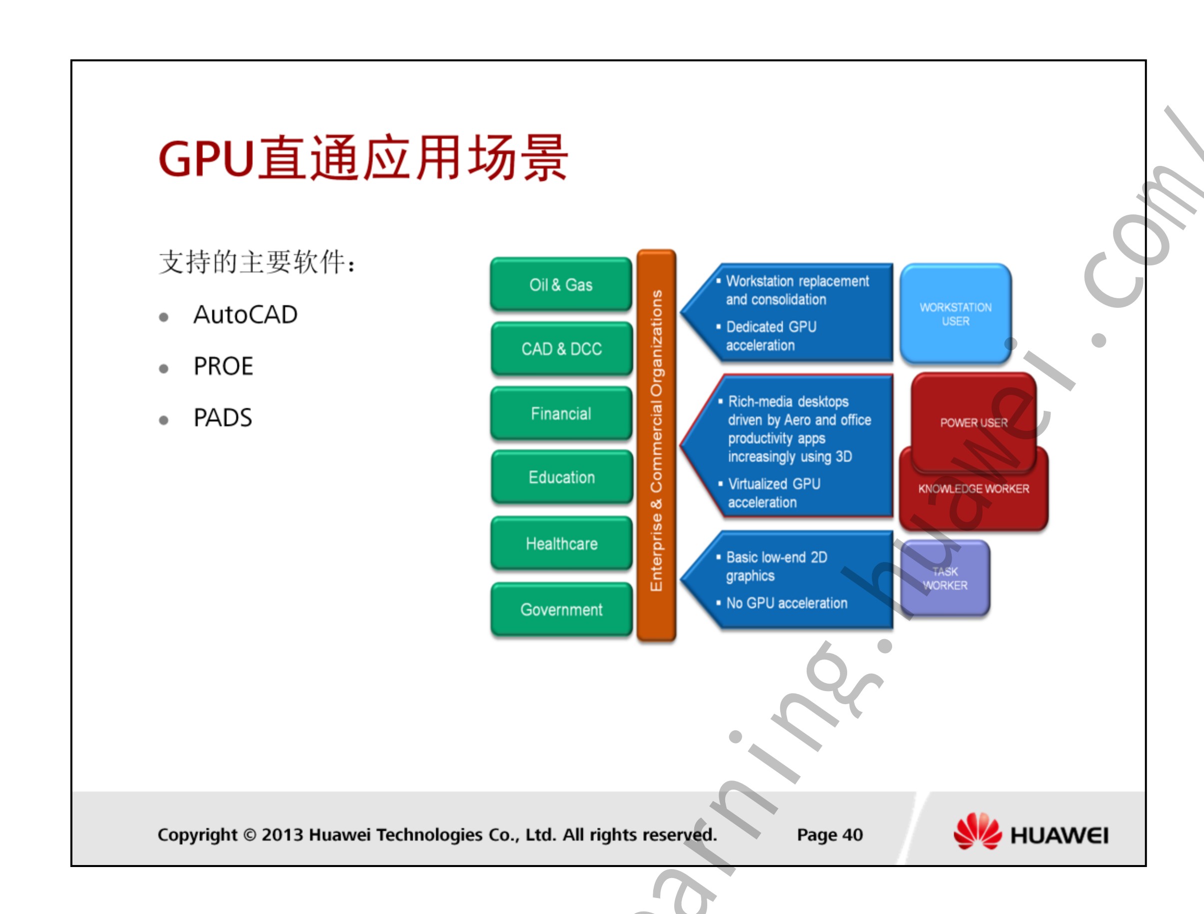


目录

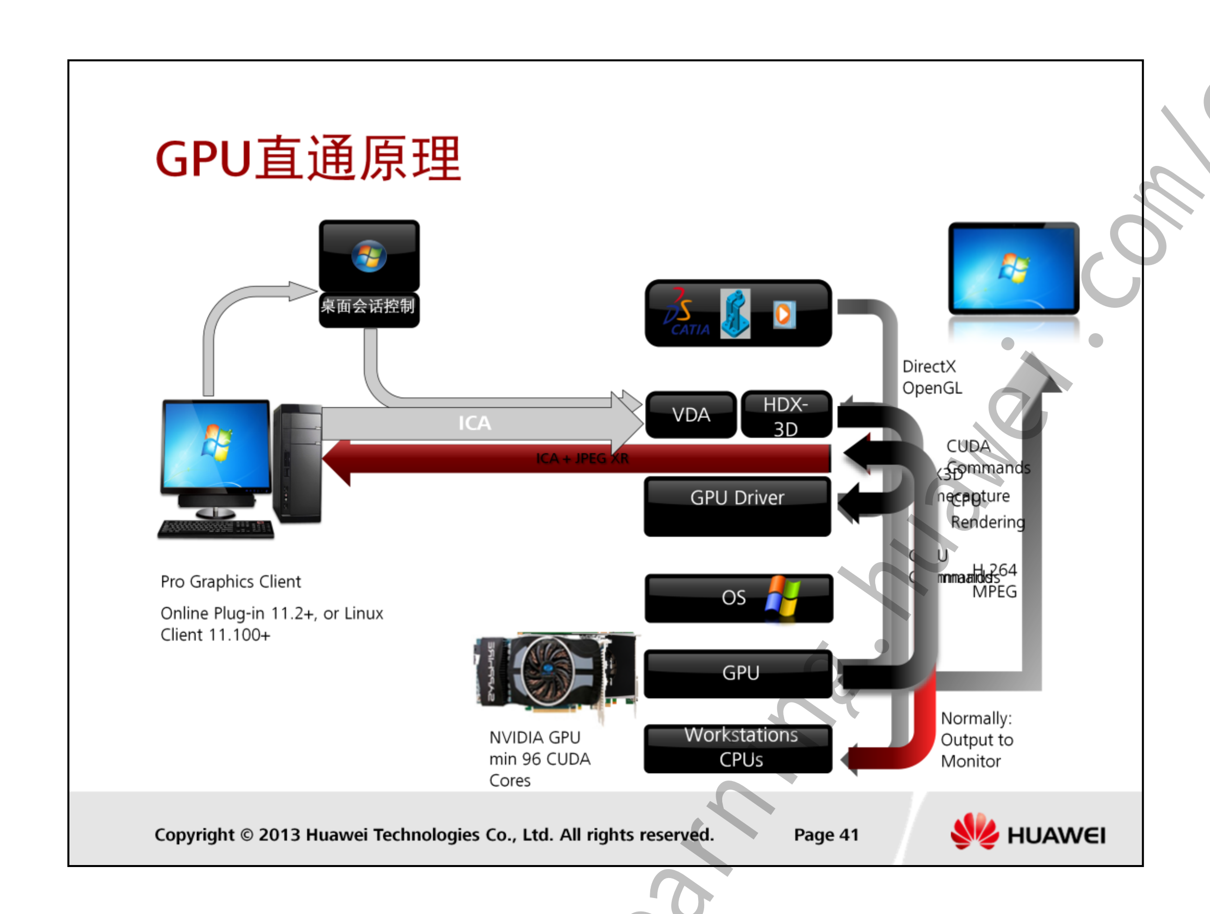




- 通过vt-x和vt-d虚拟化技术，虚拟机能够直接访问服务器的GPU（Graphic Processing Unit）进行高性能图形渲染。
- 通过远程桌面协议，服务器把渲染后的图形结果投递给终端，从而使桌面云获得高性能图形（复杂的2D、3D图形渲染）的能力。



- 业务场景一 Workstation user：（计算、渲染密集型）
  - 使用专业的2D/3D应用软件。
  - 此类制图软件通常对于3D接口（OPENGL/DX），个别软件有一定的接口兼容性要求。
  - 对于计算、渲染计算需求量较大，硬件方面需要具有高处理能力。
  - 具有较高显示分辨率要求。
- 业务场景二 Power user：3D图形应用场景中载用户-（计算、渲染中载）
  - 如图纸查看或部件级别编辑。
  - 用户要求除基本的2D功能外，还要具有3D硬件加速要求。
- 业务场景三 Knowledge Users：3D图形应用场景（无特殊性能要求）
  - 用户为非专业制图类用户，应用软件对于3D接口有着特殊的依赖需求，切换至虚拟桌面后仍然希望可以运行原有PC上程序，并接受一定体验的下降，如使用桌面游戏等，此类场景的对于3D接口的计算能够能够有CPU 模拟计算完成。



应用程序通过GPU原生驱动对GPU进行访问，协议代理从GPU Frame buffer中获取像素信息，压缩处理后传递客户端，由客户端进行还原显示。

- Client connects to DDC via WI
- DDC talks to VDA and VDA is waiting for Client`s ICA session
- Clients receive all information from DDC / WI and connects directly to VDA.
- The 3D app talks to the Displaydriver via OpenGL / DirectX
- The Driver talks to the GPU with GPU Commands
- GPU will normally deliver the finished rendered picture to the monitor
- HDX3D component capture the finished pictures
- If a Nvidia card with enough Cuda Cores is available HDX3D will generate a H.264 MPEG video via CUDA commands.
- GPU renders the video and bring out to the client in a ICA + H.264 Mpeg.
- Pro Graphics Client will decode the video and "play" the stream on his monitor
- If we don't have a Nvidia or not enough Cuda Cores or we press the 2D Drawing button HDX3D will generate a JPEG eXtended Rage stream with CPU rendering and deliver to the Client
- Pro Graphics Client, Online Plugin 11.2 and above and Linux 11.100 and above will decode the video and play the stream on his monitor.

GPU直通策略设置

- 播放高清视频或游戏
  - 推荐客户端采用PC，使用CPU深度压缩。
- 普通2D/3D制图
  - 推荐客户端采用TC，使用CPU压缩。



增加备注说明

系统规格

规格类别	详细描述
服务器	• RH2288V2/OSCA，典型配置CPU为2680
显卡	• RH2288 V2：支持NVIDIA Q2000*2 • OSCA ： Q2000*4 或Q4000*2
客户端	• PC软终端 • 如采用瘦客户端，通过POC测试确认用户可接受体验程度
虚拟桌面	• Win7/XP 32位，4U/4G • Win7 64位，8U/8G
VDA软件版本	• XenDesktop5.6 FP1及以上
Receiver软件版本	• Windows13.3、linux 12.1
3D接口	• OpenGL/DirectX
虚拟桌面分配方式	• 固定分配或动态池



增加备注说明

虚拟桌面发放



- 在服务器上安装好显卡。
- 制作用户虚拟机模板，带HDX 3D PRO的XenDesktop5.6 FP1及以上版本的VDA。
- 在FusionAccess Portal上，通过模板创建虚拟机。
- 在FusionCompute Portal上，搜索出GPU资源，分配给指定的虚拟机。
- 在FusionAccess Portal上，查询指定的虚拟机，如果已有GPU显卡，分配给用户。



增加备注说明



目录





4. 应用虚拟化



XenApp产品概述

- XenApp是一套按需应用交付解决方案:
  - 在数据中心对应用程序进行集中控制和管理。
  - 向不同地域、使用不同终端设备的用户提供虚拟应用服务。
  - 可以降低管理成本，提高IT向分散用户交付应用的响应速度，加强应用和数据的安全性。
- XenApp虚拟化应用发布技术核心是ICA协议:
  - 通过ICA虚拟通道，将运行在数据中心服务器上的应用的输入输出数据重定向到远端客户端机器的输入输出设备上。
  - 与在客户端安装软件相比，感觉不到任何操作上的改变。

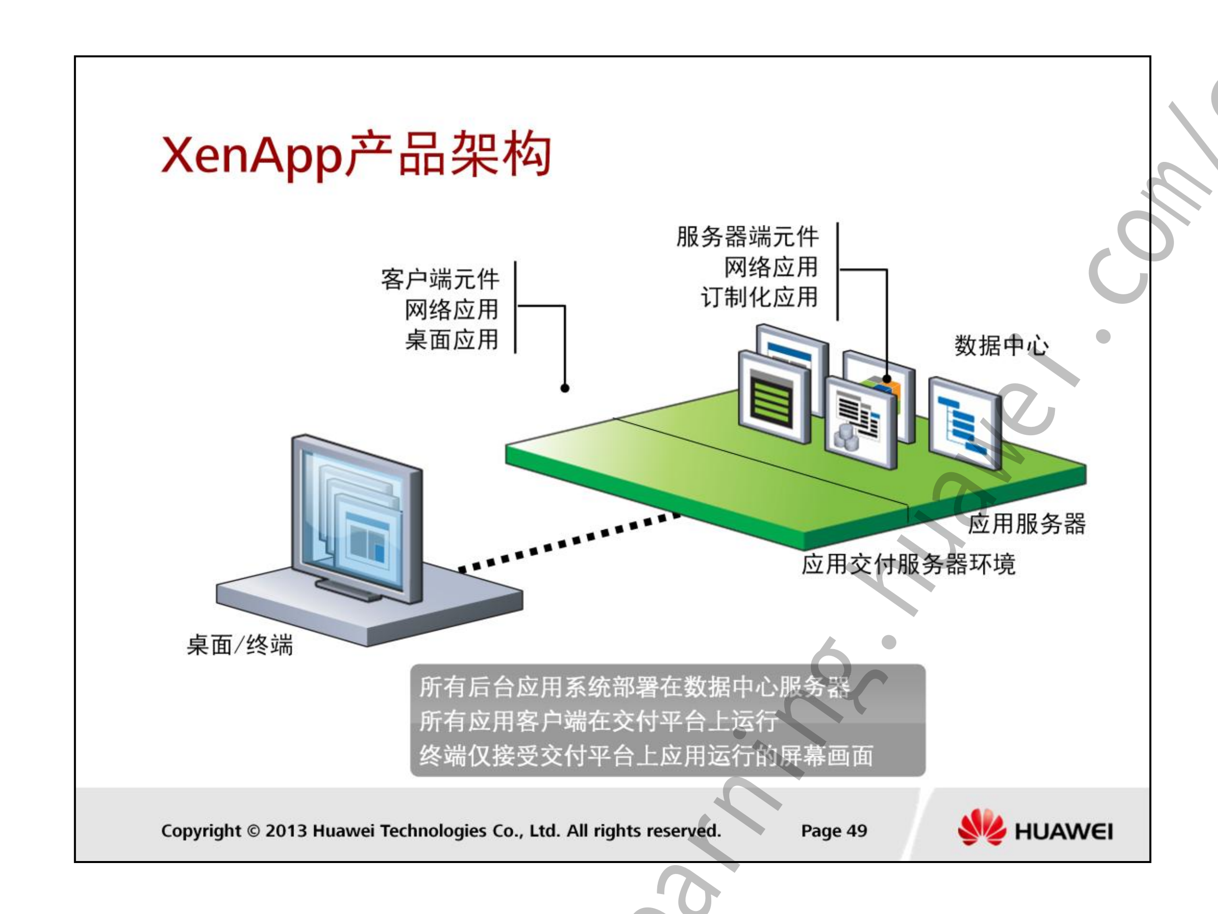
 Page 47



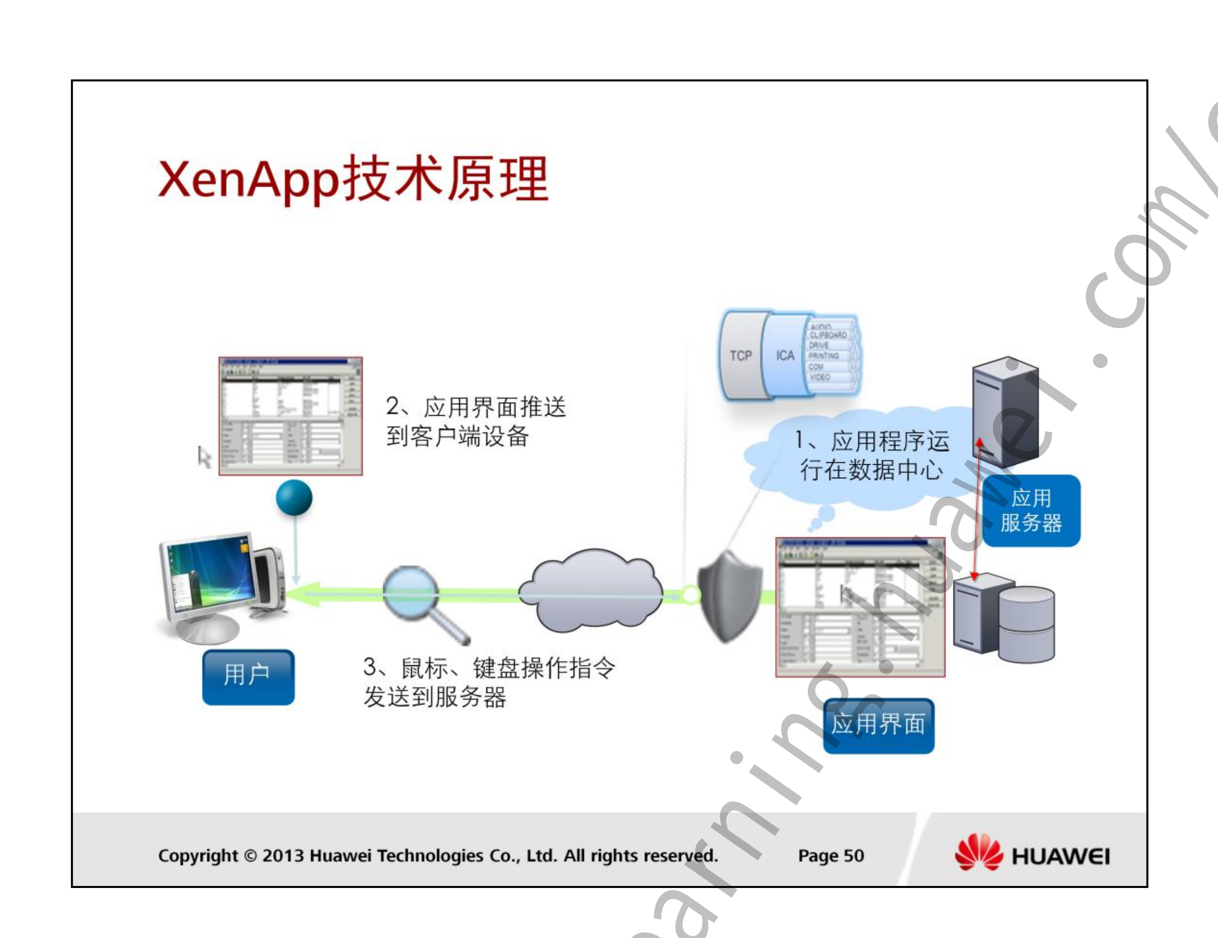


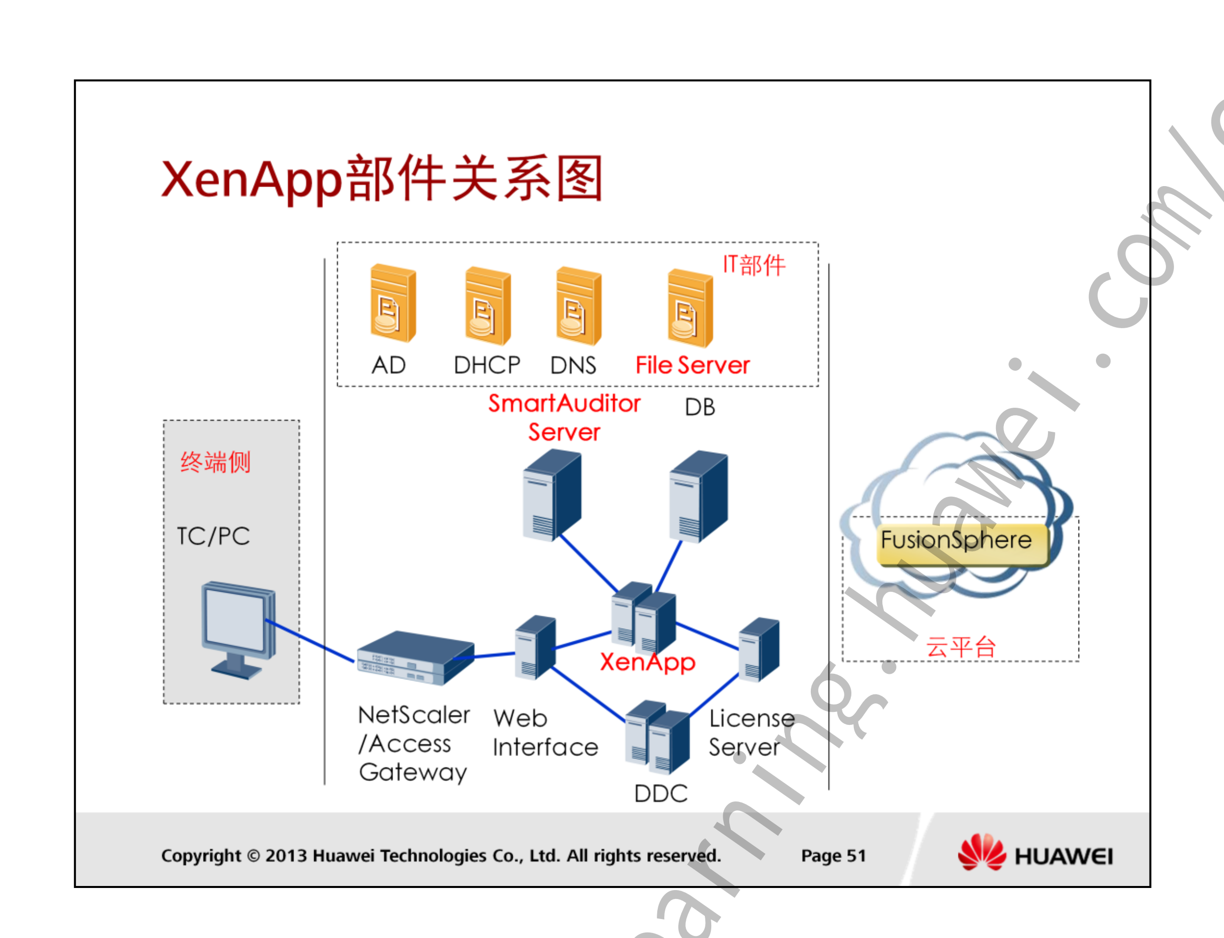
目录





- 应用虚拟化拓展了 IT 对Windows 应用进行集中管理并交付到客户端设备和服务器的能力。
- 应用虚拟化将应用和数据安全地保存在数据中心。只需传送鼠标操作和键盘敲击数据以及接收屏幕刷新数据，用户就可以通过网络访问应用。


XenApp技术原理
TCP
ICA
2、应用界面推送
到客户端设备
1、应用程序运
行在数据中心
应用
服务器
用户
3、鼠标、键盘操作指令
发送到服务器
应用界面
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 50
HUAWEI


XenApp部件关系图
IT部件
AD
DHCP
DNS
File Server
SmartAuditor
Server
DB
终端侧
TC/PC
FusionSphere
云平台
XenApp
NetScaler
/Access
Gateway
Web
Interface
License
Server
DDC
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 51
HUAWEI

XenApp部件与虚拟桌面部件比较

部件	虚拟桌面	虚拟应用	是否可共用
IT部件（AD、DNS、DHCP等）	√	√	是
终端部件（TC）	√	√	是
Web Interface	√	√	是
License server	√	√	是（用于虚拟应用时，还要兼任TS license 服务器）
DDC—VDA	√	X	否（虚拟桌面专有）
XenApp	X	√	否（虚拟应用专有）
File Server	X	√(可选)	否（虚拟应用专有，Profile重定向功能要求，未使用则可以不部署）
NetScaler	√	√	是
DB	√	√	是



XenApp服务器

- 按功能来分，XenApp组件可以分为三类：
  - Data Collector：即数据收集器，维护farm中的动态数据，用户接入时由Data Collector决定哪台XenApp worker为用户提供服务。
  - XML service：充当Web Interface 与Data Collector的中介。
  - XenApp Worker：最终为用户提供虚拟应用服务的服务器，承载应用程序和共享桌面供用户访问。

 Page 53



- 按功能来分，XenApp可以分为三类：
  - Data Collector：即数据收集器，维护farm中的动态数据，例如服务器负载、会话状态、连接的用户和许可证使用情况等。用户接入时由Data Collector决定哪台XenApp worker为用户提供服务。
  - XML service：充当Web Interface 与Data Collector之间的中介。从 Web Interface 接收用户凭据，并查询服务器场以获取用户有权访问的已发布应用程序列表。并返回给给Web Interface，在接收到用户启动应用的请求时，会将用户请求信息转给Data Collector，Data Collector选定当前连接最佳的服务器后，由XML service将该服务器的地址返回给Web Interface。
  - XenApp Worker：最终为用户提供虚拟应用服务的服务器，承载应用程序和共享桌面供用户访问。

License Server

- XenApp license server
  - 当用户访问XenApp发布的应用时，XenApp服务器需要到license server上检查是否有足够的XenApp license。
- Remote Desktop server license server
  - 当用户访问XenApp服务器时，需启动一个终端服务连接，要到license server上检查是否有终端服务license。



HUAWEI

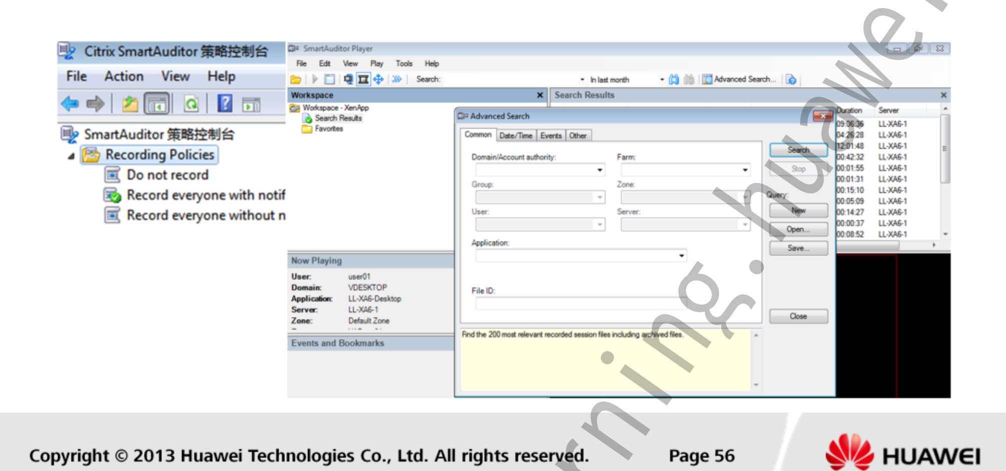
File Server

- File server存储用户的profile文件信息以及用户的个人数据。
  - 解决方案配套使用NAS部署文件服务器。
  - 使用文件夹重定向的方法来存储用户的个人数据，当普通用户使用XenApp服务器上的应用并保存数据时，只允许用户将数据保存至“文档”和“桌面”，将用户的“文档”和“桌面”目录重定向至File Server上。
  - 使用windows组策略将XenApp服务器的本地磁盘锁定，只允许管理员访问。



SmartAuditor Server

- 提供智能审计服务，任何用户使用XenApp发布的应用可以被全程监控，用户的操作行为及显示器上的内容变化可以通过ICA协议存放到磁盘上，然后在需要的时候可以回放。



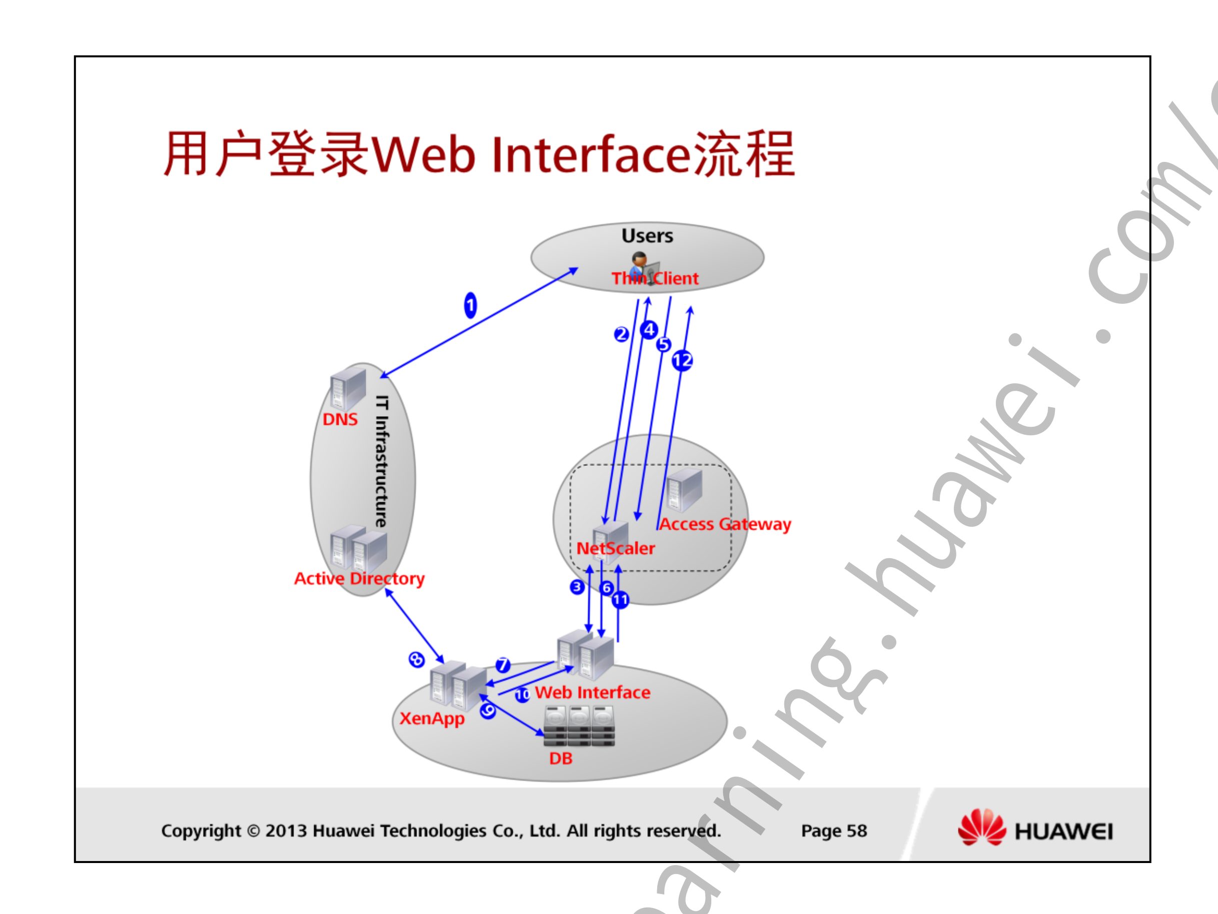
HUAWEI



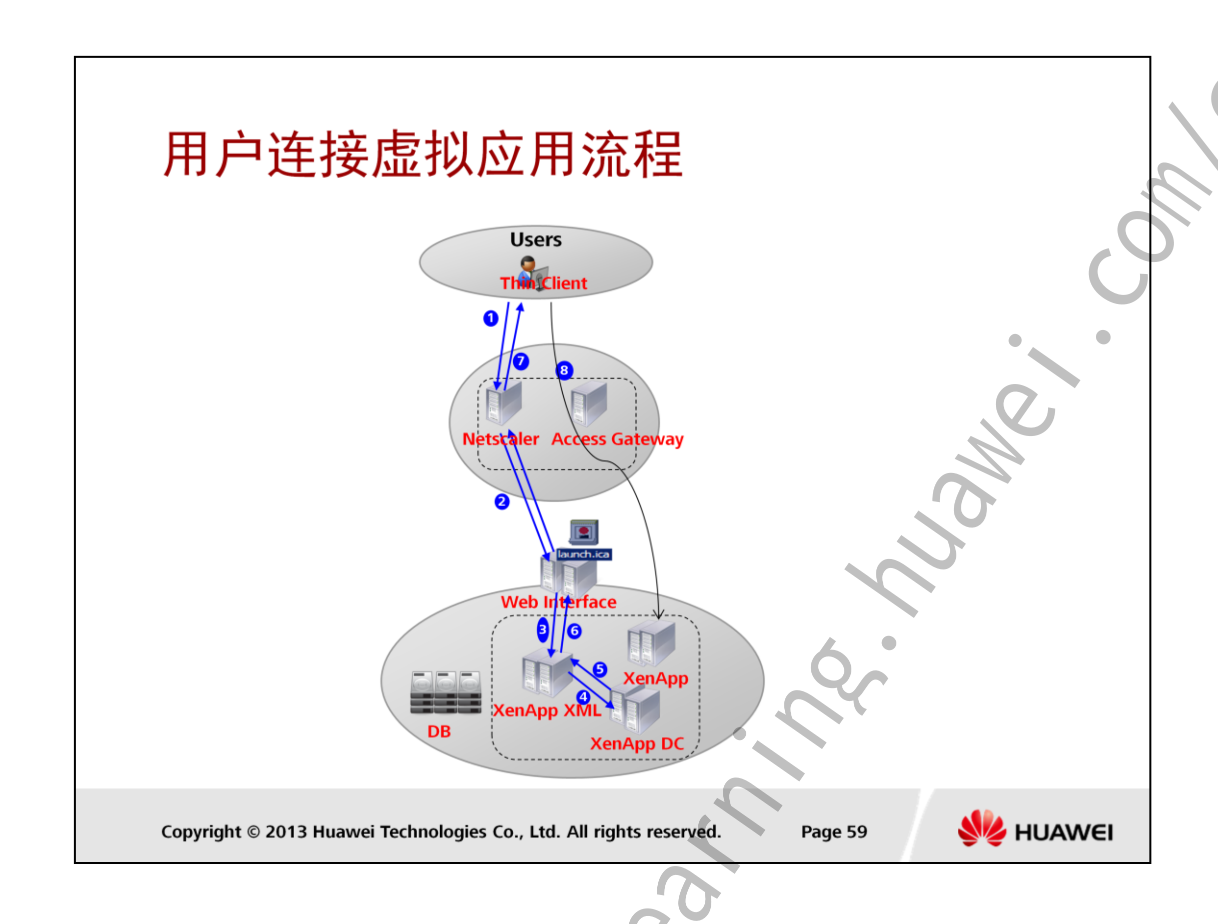
目录

4. 应用虚拟化





1. 用户在TC上输入LB域名，TC到DNS查询LB的IP地址；DNS返回LB的IP地址。
2. TC将登录请求发送到NetScaler 。
3. NetScaler将登陆请求转发给WI，WI将登陆页面发送给NetScaler 。
4. NetScaler将登陆页面发送给TC。
5. 用户输入用户名和密码，TC将接入请求发送给NetScaler。
6. NetScaler将用户名和密码发送给 WI。
7. WI将用户名和密码发送给XenApp-XML。
8. XenApp-XML将用户名和密码发送给AD请求认证，AD返回认证成功 。
9. XenApp-XML从DB查询用户的应用列表。
10. XenApp-XML将用户的应用列表返回给WI。
11. WI 将用户虚拟应用列表展现在Web页面上，同时 WI将Web页面转发给 NetScaler。
12. NetScaler将页面内容转发给终端TC显示。



1. 用户在Web页面中点击发布给自己的应用或者共享桌面，请求发送到NetScaler。

2. NetScaler将请求转发到WI。

3. WI将连接请求发送到XenApp-XML。

4、XenApp-XML 向XenApp Data Collector(简称XenApp DC)报告接入请求。

5、XenApp DC根据各个XenApp服务器发布的应用及负载状况决策由哪台XenApp服务器来给用户提供服务，并将该XenApp服务器的IP地址返回给WI。

6.WI根据XenApp的连接信息生成ICA文件，将其返回给NetScaler。

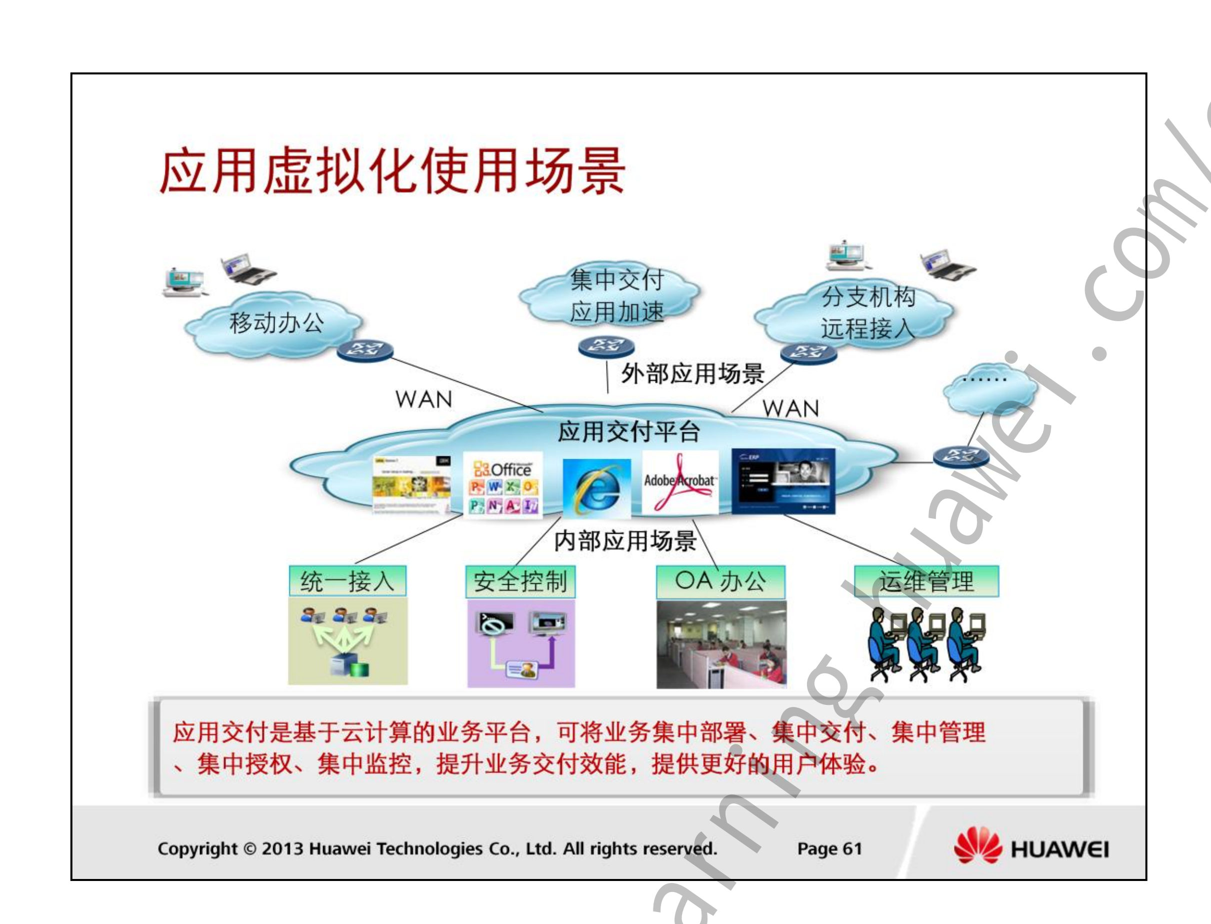
7.Netscaler将ICA文件转发给终端。

8.终端收到ICA文件后，对其进行解析，ICA文件中已指示了Access Gateway的域名，终端将ICA请求直接发送到AG。AG转发给相应的XenApp服务器，XenApp服务器接收到ICA请求，与终端建立连接。



目录




应用虚拟化使用场景
移动办公
集中交付
应用加速
分支机构
远程接入
外部应用场景
WAN
WAN
……
应用交付平台
Office
Adobe Acrobat
内部应用场景
统一接入
安全控制
OA 办公
运维管理
应用交付是基于云计算的业务平台，可将业务集中部署、集中交付、集中管理、集中授权、集中监控，提升业务交付效能，提供更好的用户体验。
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 61
HUAWEI

应用交付使用场景分析

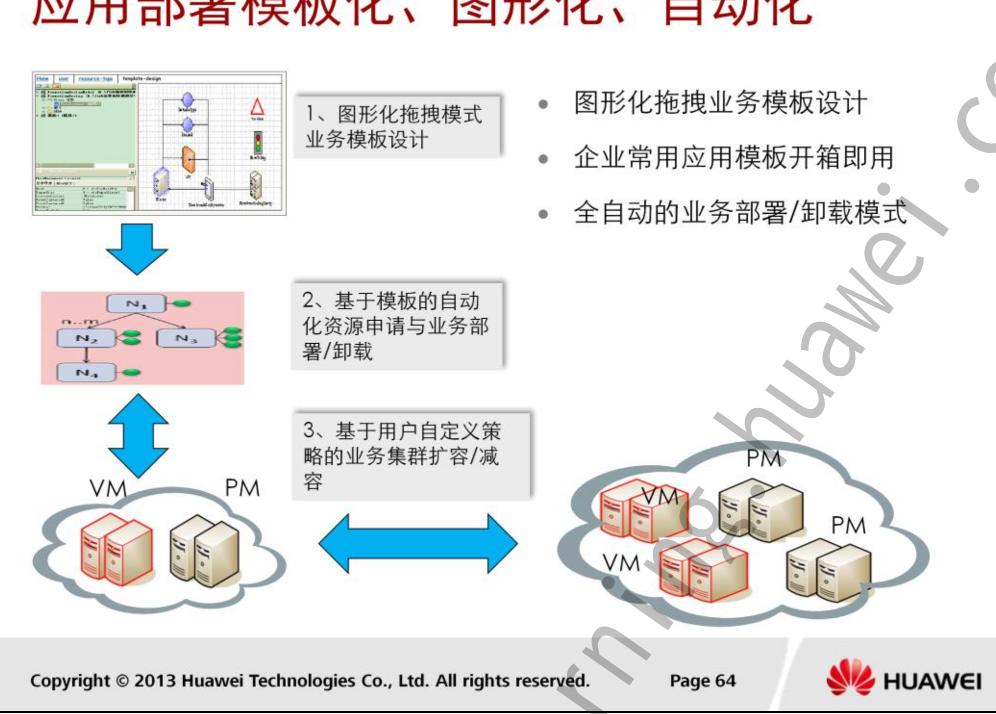

优化体验
✓ 移动随时随地办公
✓ 统一简化的IT访问
✓ 单点登录多个应用
✓ 第三方门户集成
集中管理
✓ 全球化IT业务系统整合
✓ 安全业务环境下集中上网
✓ 业务系统集中管理运维
✓ 远程网络运维管理
✓ 远程应用交付与业务访问
✓ 海外分支机构远程访问
✓ ERP、CRM等企业IT交付
✓ 传统应用系统的迁移
✓ 柜员环境前后台业务分离
✓ 第三方外包伙伴业务访问
✓ 区域业务集中与应急恢复
✓ 基于安全策略的应用交付
应用交付
安全控制


HUAWEI



目录





- 应用自动部署：用户通过已发布的服务模板进行应用自动部署，自动地创建虚拟机，自动地在虚拟机上安装应用软件，自动地建立网络连接，自动地建立应用软件间的依赖关系。
- 图形化拖拽业务模板设计
  - 通过所见即所得的方式设计业务部署模板，极大的降低了业务部署设计难度
- 企业常用应用模板开箱即用
  - 系统预集成企业常见基础应用部署模块，提供开箱即用的IT服务
- 全自动的业务部署/卸载模式
  - 一键式业务部署、回收，可以快速实现企业IT服务发放及资源回收

应用自动部署流程

step1
创建组织资源

step2
创建并发布虚拟机模板

step3
注册并发布软件包

step4 创建并发布服务模板

Step5 使用服务模板，创建应用

- step1包括创建组织，组织VDC，组织网络。
- step4包括创建服务目录，创建服务模板，发布服务模板。


STEP1：创建组织
添加组织
组织名称:
huawei
由汉字、字母、数字、下划线组成，长度范围是 1 个～ 20 个字符。
描述:
组织管理员
用户名:
huaweiadmin
由数字、字母、下划线组成，长度范围是1个～20个字符。
密码:
确认新密码:
添加
取消
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 66
HUAWEI


STEP1：创建组织VDC
首页
故障管理
系统管理
权限管理
资源管理
创建组织VDC
基本信息
选择资源集群
资源配额
确认信息
配置基本信息
* 名称:
huaweivdc
长度范围1～128个字符。
描述:
长度范围0～1024个字符。
下一步
取消
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 67
HUAWEI

STEP1：创建组织网络

  HUAWEI

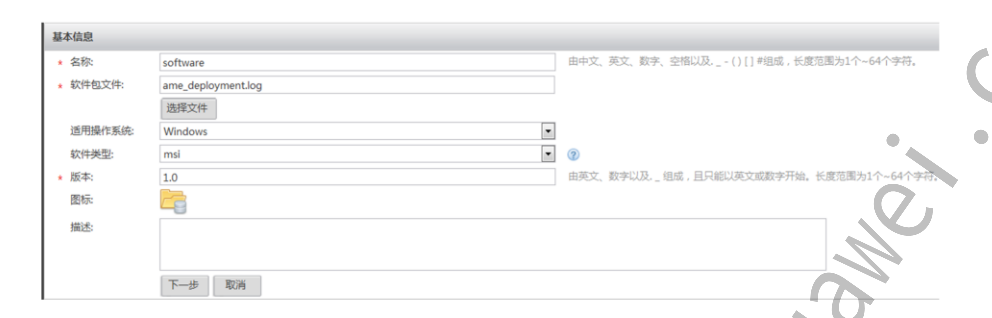
STEP2：创建并发布虚拟机模板



说明：虚拟机模板发布后，在服务模板页面才能够看到并使用。



STEP3：注册并发布软件包



说明：名称和图标会显示在服务模板创建页面供用户选择。
发布软件包和发布模板相似。



STEP4：创建并发布服务模板（1/3）





创建好的服务模板只是一个草稿，只发布之后才能用来创建应用。

好处：提供友好的可视化界面，让使用者通过简单的拖拽，再配合简易的参数输入，来实现服务模板的创建。

 Page 71 HUAWEI

STEP4：创建并发布服务模板（2/3）

选中虚拟机模板后，可修改虚拟机模板规格。

服务模板部件之虚拟机模板

HUAWEI

STEP4：创建并发布服务模板（3/3）

服务模板部件之伸缩组

STEP5：使用服务模板，创建应用（1/4）

huawei	组织			ame		2013-04-02 15:13:29 U...	wp
Test	公有	发布			VT_Test	2013-04-02 15:13:47 U...	wp
haobinbin	组织			ame		2013-03-30 10:11:32 U...	ame

创建应用

服务目录管理页面，选择服务模板，创建应用

HUAWEI

STEP5：使用服务模板，创建应用（2/4）

基本信息

* 应用名称: huaweiapp 由中文、英文字母、数字、中划线、下划线及空格组成，长度范围为1个~64个字符。

* 组织: huawei

* 组织VDC:

	名称	资源总数	可用资源	描述
◎	huawei_vdc	CPU(GHZ):10.0,Memor...	CPU(GHZ):10.0,Memor...	

此处选择的是创建虚拟机的计算资源信息

描述:

下一步 取消

STEP5：使用服务模板，创建应用（3/4）

配置应用参数

* 网络选择：

网络	组织网络
DefaultNetwork_1	hauwei_net 选择

此处选择的是创建虚拟机的网络资源信息

公共参数：

参数名称	参数值	参数描述
	没有记录	

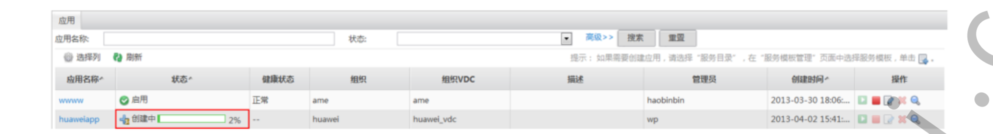
上一步 下一步 取消


STEP5：使用服务模板，创建应用（4/4）
配置管理员
管理员:
可选用户
用户名
用户类型
描述
huaweiadmin
业务管理员
admin
系统管理员
default user
已选用户
wp
系统管理员
上一步
下一步
取消
提交成功，正在创建资源...
继续创建
关闭
注：可在 应用管理 查看进度
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 77
HUAWEI



- 业务管理员和系统管理员可以查看应用拓扑的详细信息，包含应用所属于的虚拟机的状态及告警信息。可以通过VNC登录的方式进入虚拟机进行操作，同时在操作栏中提供虚拟机常用的操作，满足业务管理或系统管理快速的查看应用的信息和处理故障。

应用管理



此页面提供应用管理功能:

- 应用创建进度查看，应用健康状态查看，应用详情查看。
- 应用的基本操作，启动，挂起，修改，删除，查看。





目录



弹性伸缩介绍

- 弹性策略类型
  - 组内伸缩
  - 组间伸缩
  - 计划任务

 Page 81 

- 弹性伸缩：根据策略进行资源的合理分配，在满足不同应用需求的前提下，达到资源的最大化利用，提高资源的利用率。其主要方法为通过配置不同的策略，监控VDC（逻辑集群）内的计算资源的各项指标（如CPU RATE），动态调整资源在各应用间或者应用内的分配，实现资源的分时复用，以提高资源的利用率，减少投资成本。
- **组内自动伸缩策略：**
  - 组内自动伸缩是针对单独的应用而言的。应用在运行过程中，组内自动伸缩策略根据应用的负载动态的调整应用使用的资源，这里的动态调整主要分为伸和缩。伸是指当一个应用资源负载较高时，系统自动的给这个应用动态的添加虚拟机，并且安装应用软件，以降低应用的整体资源负载，使应用能够健康的运行。缩和伸是相对的，当应用的资源负载很低时，系统可以自动的减少应用使用的虚拟机，释放相应的资源，以达到应用间资源的有效复用和节能减排的目的。
- **组间资源回收策略：**
  - 组间资源回收策略指的是，当系统资源不足的情况下，系统可以根据组间设置的资源复用策略， 优先使优先级高的应用使用资源，使优先级低的应用释放资源，以供优先级高的应用使用。

弹性伸缩介绍

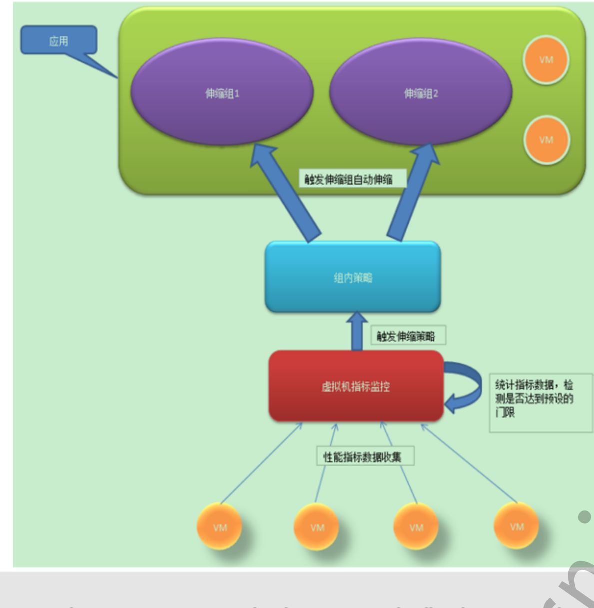
- 弹性策略类型
  - 组内伸缩
  - 组间伸缩
  - 计划任务

 Page 82 

- **时间计划策略:**
  - 时间计划策略允许用户对于不同的应用实现资源的分时复用。用户可以设置计划策略，使得不同的应用分时段的使用系统资源，比如说白天让办公用户的虚拟机使用系统资源，到了晚间可以让一些公共的虚拟机资源做其他应用如图像渲染。

- 应用举例：监控Hadoop计算集群中Task Traker，当整个集群中CPU利用率高于80%时，自动增加Task Traker节点，加速任务执行。当一段时间内，集群的平均CPU利用率小于10%时，自动减少Task Traker节点。

应用弹性伸缩 - 组内伸缩

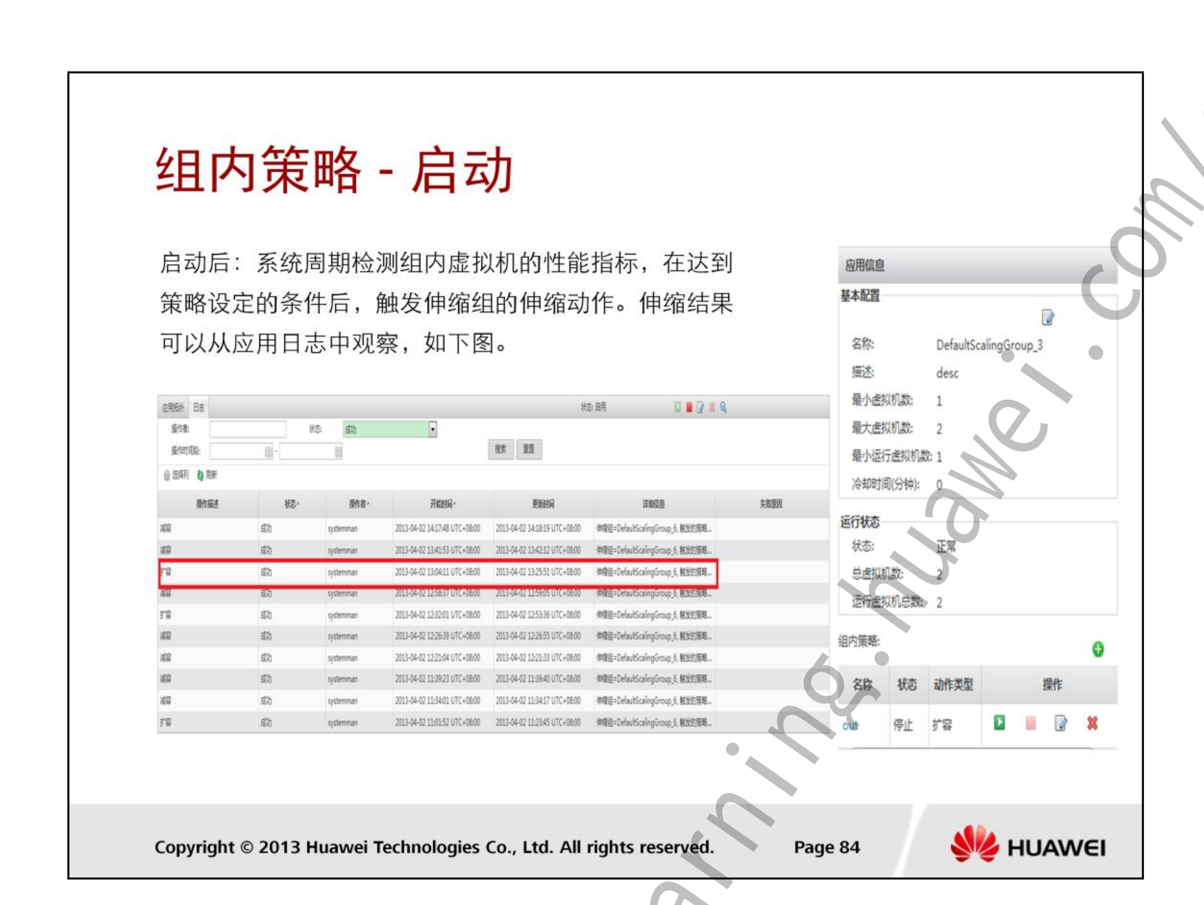


- 伸缩组：一组适用于相同伸缩策略的虚拟机的集合
- 组内策略：控制伸缩组如何伸缩的规则
- 虚拟机指标监控：周期收集虚拟机的性能指标数据，并计算是否触发组内策略。

Page 83



- 组内策略：控制伸缩组如何伸缩的一条规则，包含参数：
  - 指标及门限
  - 统计周期
  - 动作
  - 步长
  - 冷却时间


组内策略 - 启动
启动后：系统周期检测组内虚拟机的性能指标，在达到策略设定的条件后，触发伸缩组的伸缩动作。伸缩结果可以从应用日志中观察，如下图。
应用信息
基本配置
名称: DefaultScalingGroup_3
描述: desc
最小虚拟机数: 1
最大虚拟机数: 2
最小运行虚拟机数: 1
冷却时间(分钟): 0
运行状态
状态: 正常
总虚拟机数: 2
运行虚拟机总数: 2
组内策略:
名称
状态
动作类型
操作
停止
扩容
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 84
HUAWEI

应用弹性伸缩 - 组间策略

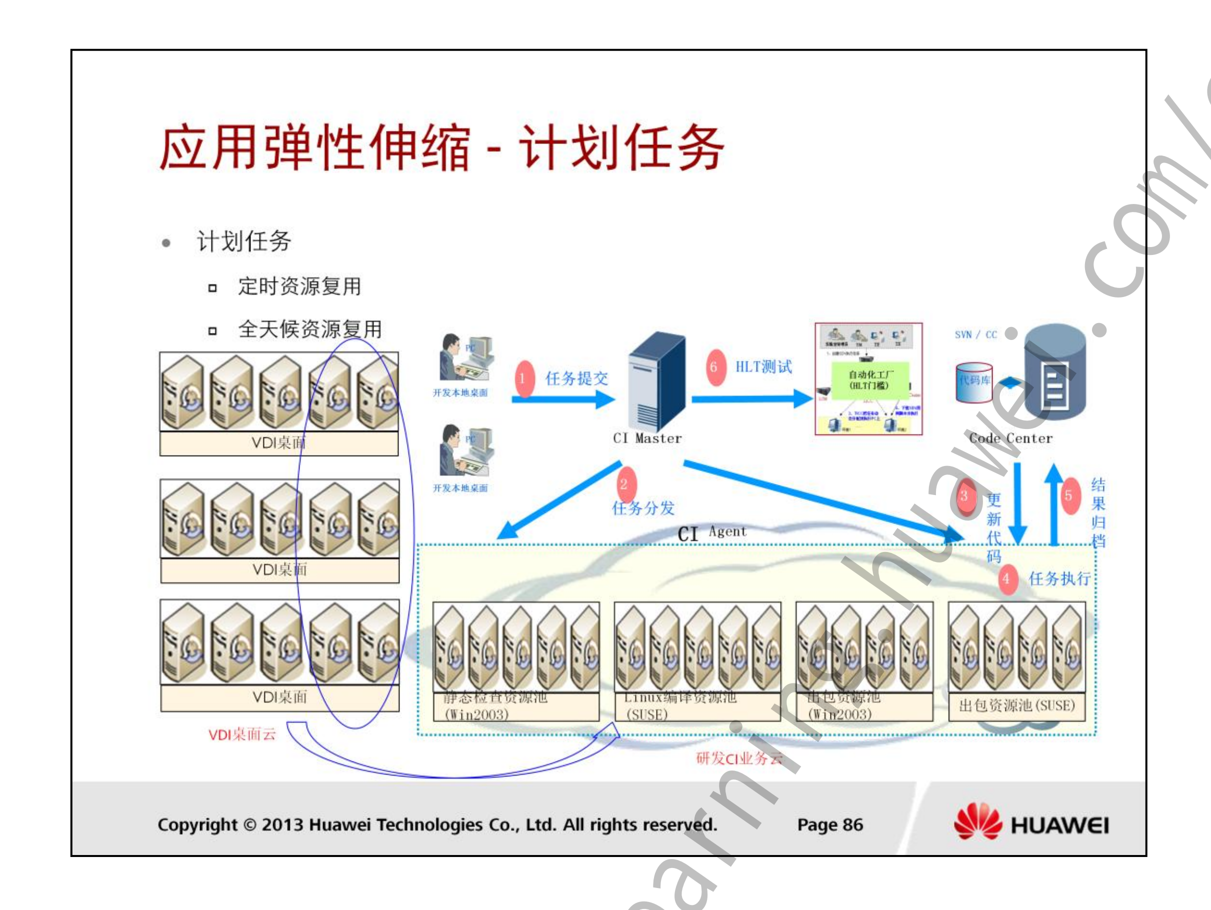
- 组间资源共享策略：在一个集群下运行的各个应用之间资源占用和共享的关系。可以配置集群的预留资源阈值，以及各应用的资源门限和分享比例。
- 组间资源共享策略对应一个集群，一个集群可以运行多个应用。每个集群对应不同的组间资源共享策略。

添加组间策略

- 名称：between_policy
- 预留CPU(MHz)：1000
- 预留内存(MB)：1000
- 描述：
- 复用配置：添加

伸缩组名称	应用名称	CPU分配最大值(MHz)	CPU分配预留值(MHz)	内存分配最大值(MB)	内存分配预留值(MB)	优先级	操作
DefaultScalingGroup_3	wwww	500	100	1000	500	高	

- 策略参数配置
  - Buffer：集群缓冲资源阀值，集群缓冲资源用于某些异常情况下的资源申请，如用户发起的VM唤醒，以及VM性能保障。
  - Reserved：资源预留，为应用保证的资源使用量。当申请资源在Reserved范围之内的，必须保证。超出Reserved的资源申请，根据系统资源情况及优先级分配。应用不使用时，这部分资源仍会保留，不会参与资源的共享和分配。
  - Large：资源的最大使用数量。应用申请的资源不能超出该限制。
  - Priority：可共享资源分配使用的绝对优先级。分为高、中、低三个等级。当发生资源不足时，高优先级可以绝对抢占中、低优先级应用超出R的资源，同样中优先级可以绝对抢占低优先级超出R的资源，默认为低。
- 组间策略触发资源回收的条件：
  - 集群空闲资源小于Buffer时
  - 应用申请的资源超过Large时
- 组间策略触发资源回收的动作：关机



●计划任务：设置应用组内策略及组间资源共享策略的执行时间，支持定时、周期或时间段执行预配置的策略，实现资源的时分复用

●定时资源复用：白天使用虚拟桌面办公，晚上不使用了释放其计算资源，系统可以使用此资源运行CI业务，到第二天早晨关闭复用资源的CI业务，VDI用户上班后可以继续使用虚拟桌面

●全天候资源复用：白天当VDI有空闲资源时，也可以拿出来给CI业务使用，当VDI用户资源不够时，自动释放CI资源，返还给VDI业务使用

计划任务 - 创建

- 触发类型：定时触发、周期触发
  - 定时触发：按照设定的日期和时间，仅触发一次
  - 周期触发：分为按天触发和按周天触发
- 启动后计划任务将按预设的时间执行

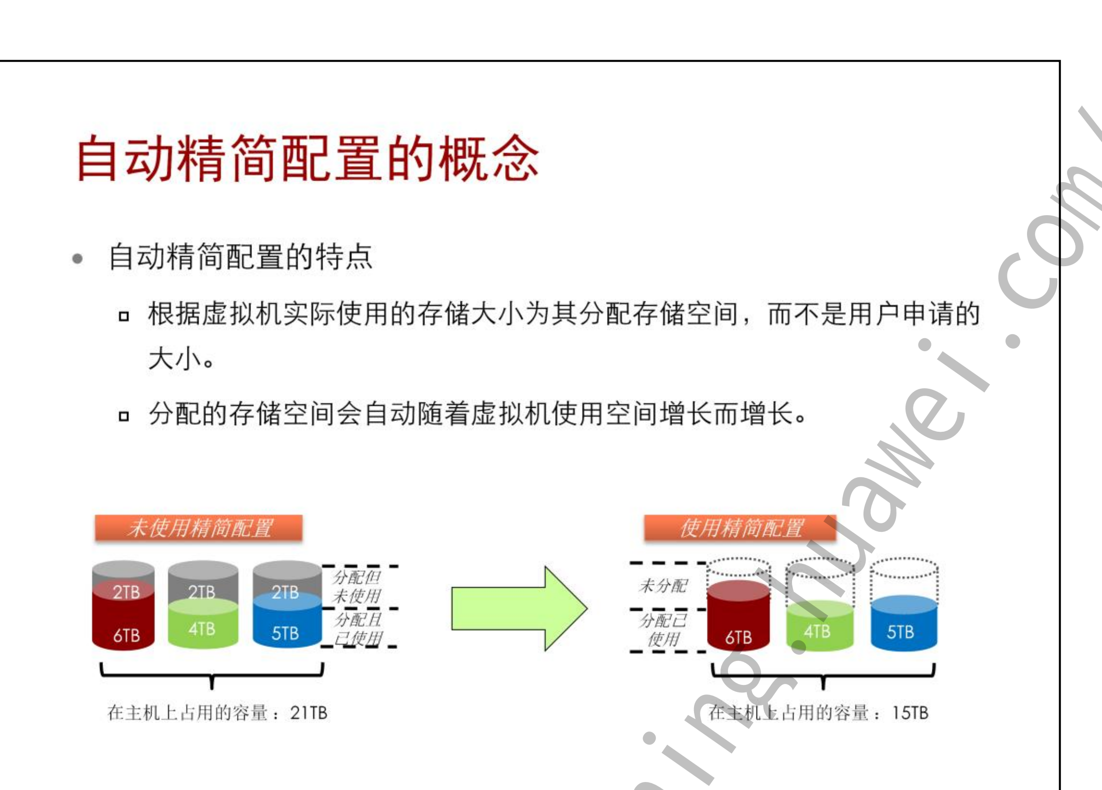


HUAWEI



目录





- 存储自动精简配置（Thin Provisioning）又名存储超分配或存储瘦分配。

自动精简配置的应用

- 支持自动精简配置的数据存储类型有3类，后续主要描述虚拟化存储的自动精简配置：
  - FusionStorage
  - Advanced SAN
  - 虚拟化存储（包括本地硬盘、共享存储和NAS存储）
- 自动精简配置的应用
  - 主机的存储需求，规划的比实际应用的多。
  - 有多种业务需求，但是各种业务对存储的需求量并不明确。
- 自动精简配置的意义
  - 降低初始投资及维护成本、提高资源利用率

 Page 90



- FusionStorage和Advanced SAN的精简配置是在存储设备上创建存储资源池，每次创建精简磁盘只分配很少的空间，随着用户写入数据，会从资源池中自动分配存储单元给精简磁盘使用
- 虚拟化存储的精简配置是通过文件系统和动态磁盘文件来实现的。动态磁盘文件会随着用户写入数据，会自动从文件系统中分配空间。

自动精简配置的空间回收

- 空间回收的必要性：
  - 自动精简配置下，磁盘的在数据存储上的占用空间会随着用户使用的增长而增长，但不会随着用户删除数据而缩减。
  - 长时间运行后，磁盘在数据存储上的占用空间会接近磁盘的规格，精简配置的效果会减弱。
- 空间回收的作用：
  - 将因删除虚拟机用户而释放的空间从数据存储上释放出来给其他虚拟机使用。
  - 管理员进行回收操作后，磁盘占用的空间可以接近用户使用的空间，提高存储利用率。



自动精简配置的使用方法

- 自动精简配置时磁盘的属性，创建磁盘时，可以设置磁盘是普通或精简
- 自动精简配置可以查询在数据存储上占用的空间，和用户已使用的空间
- 自动精简配置的回收功能

配置模式: 普通
普通
精简
不受快照

容量(GB)	实际使用容量(GB)	用户已用空间(GB)
5	2.513	4.014

所属数据存储	操作
NASdata1	

解绑定
编辑磁盘
调整容量
空间回收
磁盘备份

HUAWEI

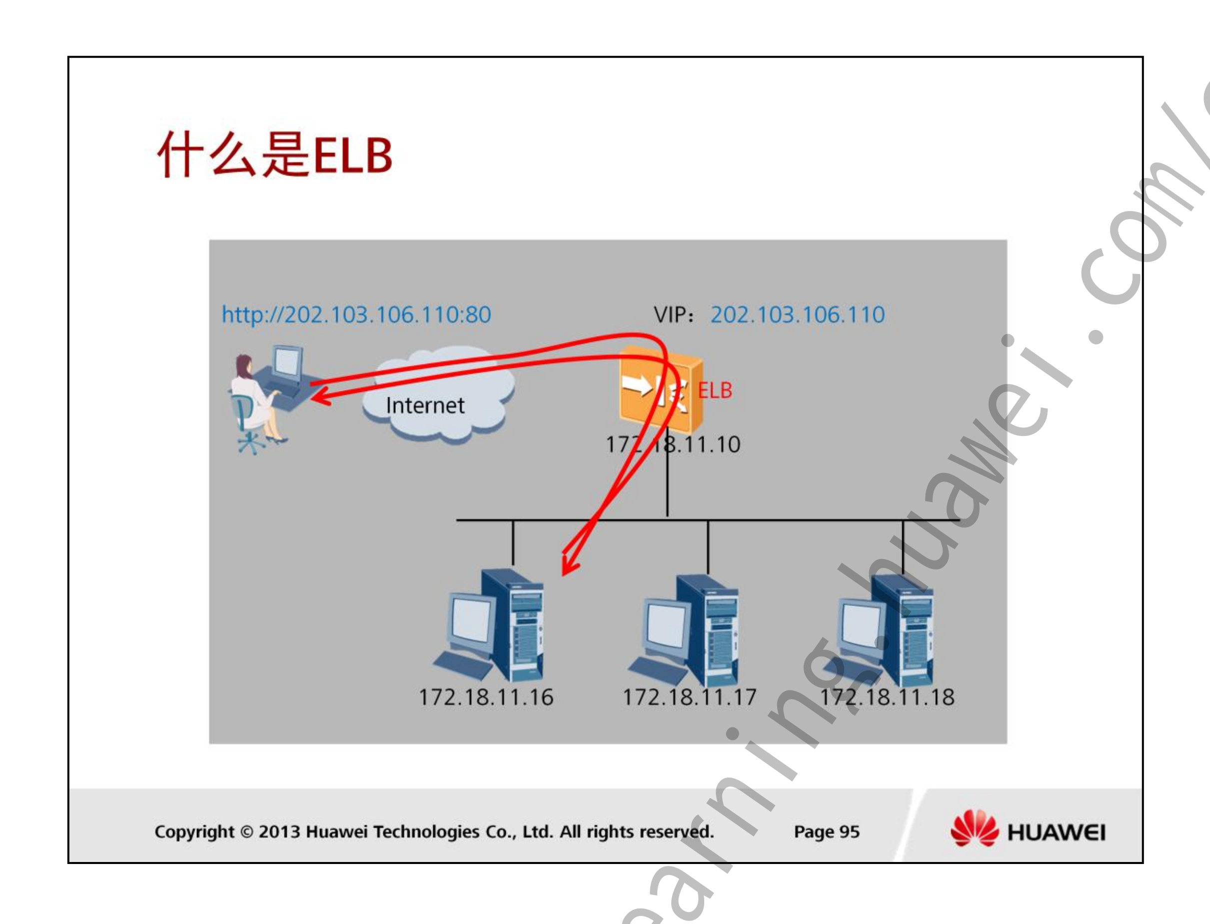


目录

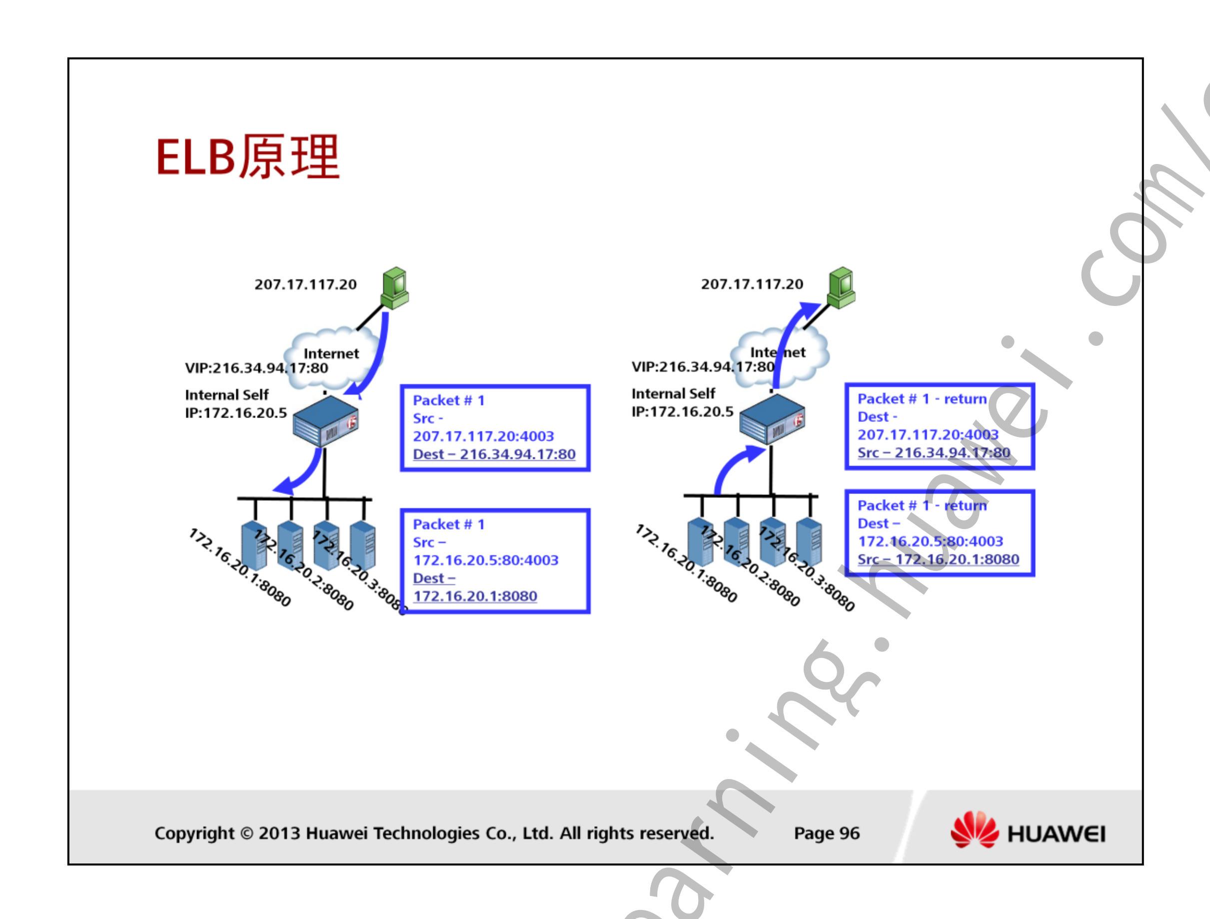



目录
8. ELB
8.1 ELB原理
8.2 ELB功能
8.3 ELB应用场景
8.4 ELB配置
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 94
HUAWEI

- ELB，弹性负载均衡



- ELB：Elastic Load Balancer，弹性负载均衡，是云提供商提供的一个网络服务
  - 自动部署：用户无需关注负载均衡器的物理部署和组网；
  - 自助服务：用户可直接在portal上按业务需求定制；
  - 简化配置、快速提供服务：用户可在3分钟之内部署负载均衡服务，缩短业务上市时间
  - 灵活：适用于私有云、公有云、混合云；



1、客户端发送请求到VIP；

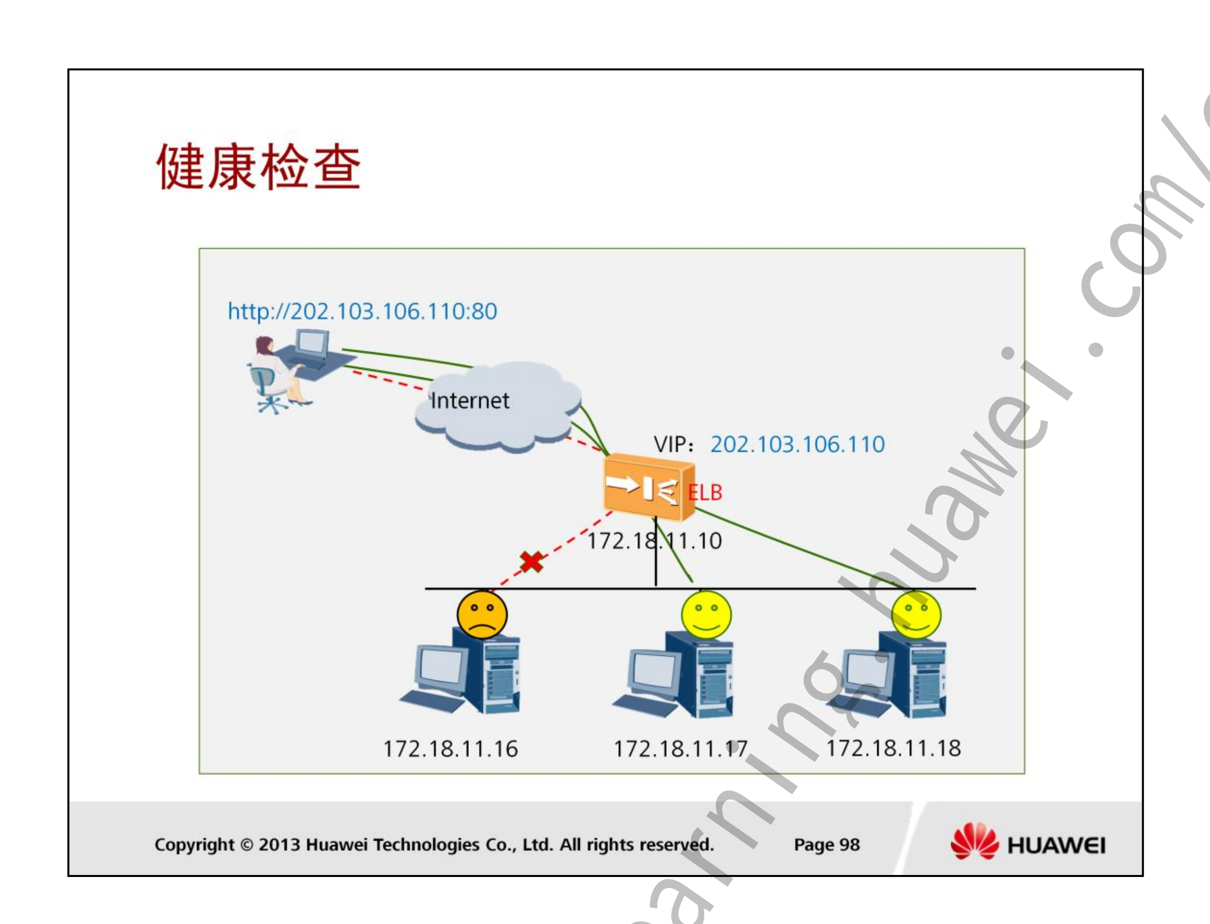
2、ELB将数据包中的目的IP改为选中的后台服务器IP地址，然后将数据包发送到后台选定的服务器；

3、后台服务器收到后，将应答包按照其路由发回到ELB；

4、ELB收到应答包后，将其中的源地址改回成VIP地址，发回客户端。







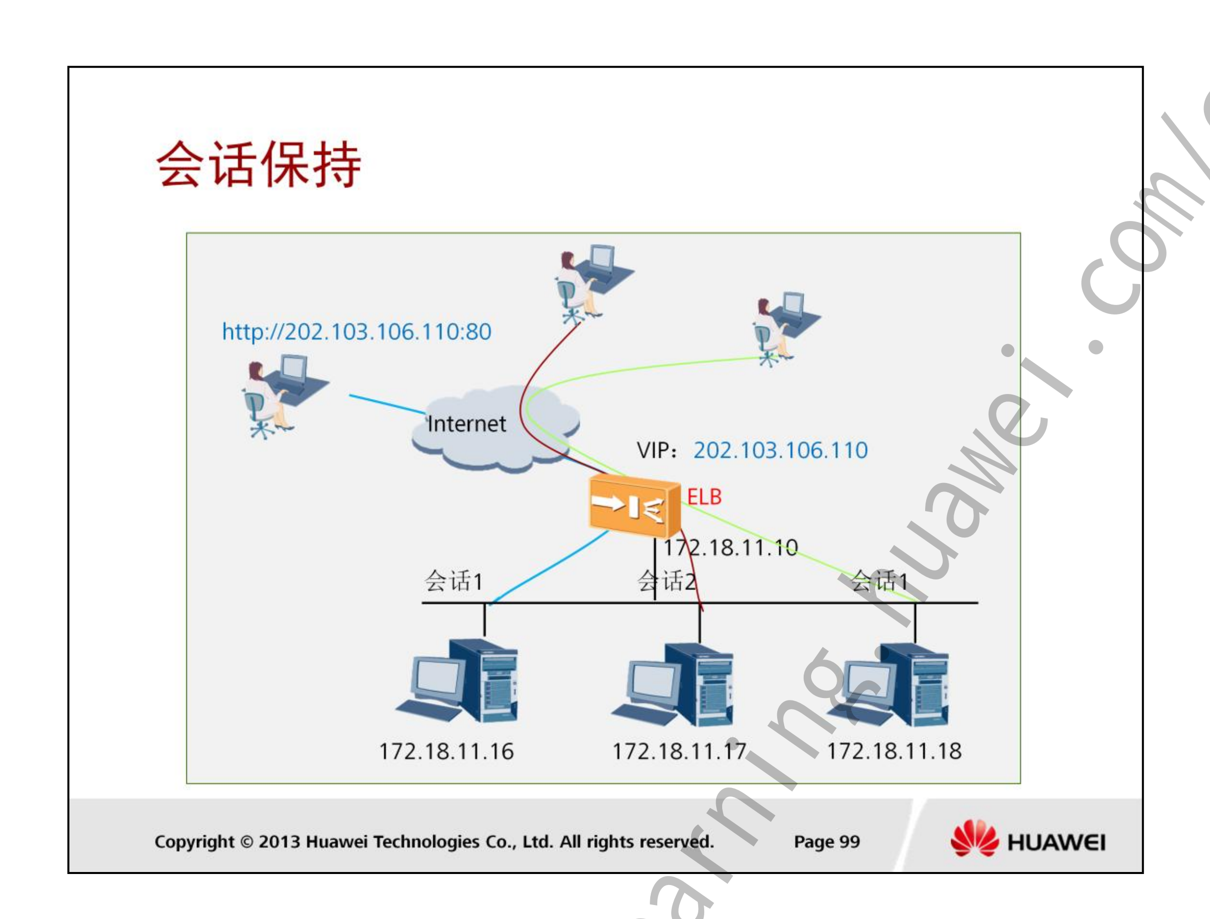
- **健康检查场景：**

  ELB在转发用户请求时，检测各服务节点的状态，将请求转发到健康的服务节点。

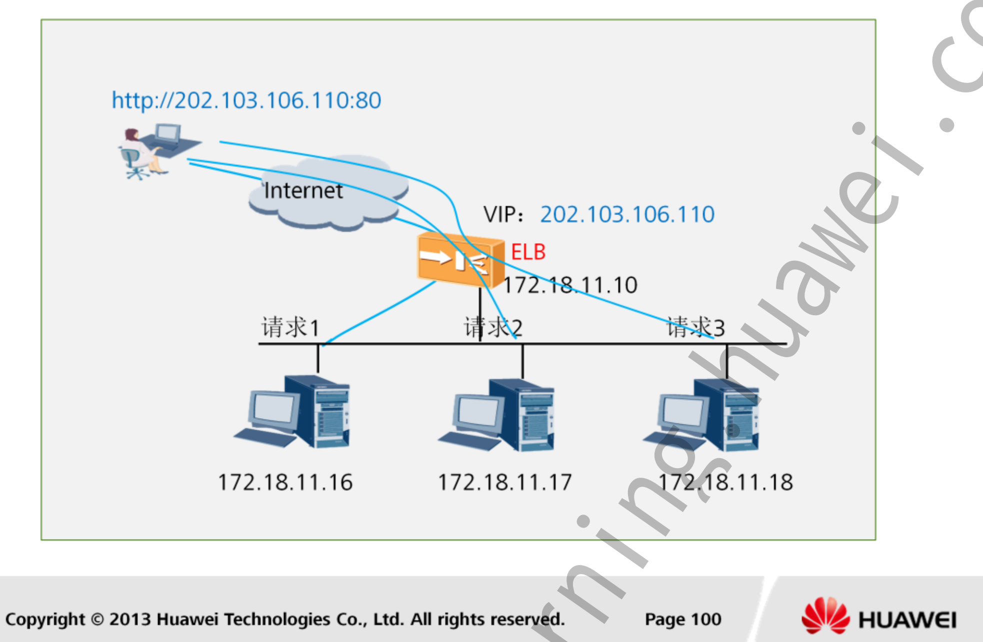
- **原理：**

  ELB定期请求web业务地址，在设定时间内收到响应，则认为服务能够提供服务；

  ELB定期通过ICMP请求后台的服务器IP地址，在设定时间内收到响应，则认为该节点能够服务。



- 会话保持:
- 用户访问具有会话的业务时，该会话信息只存在于用户初次请求的服务节点上，该会话上后续的请求，都转发到同一个节点，保证业务的可用



- 轮询：
  - 将用户的请求依次转发到不同的服务主机上
- 适用场景：
  - 适用于无状态的服务，如共享式web服务

分发算法-最小连接数算法

http://202.103.106.110:80

Internet

VIP：202.103.106.110

ELB

172.18.11.10

请求1

请求2

请求3

500 连接

200 连接

50 连接

172.18.11.16

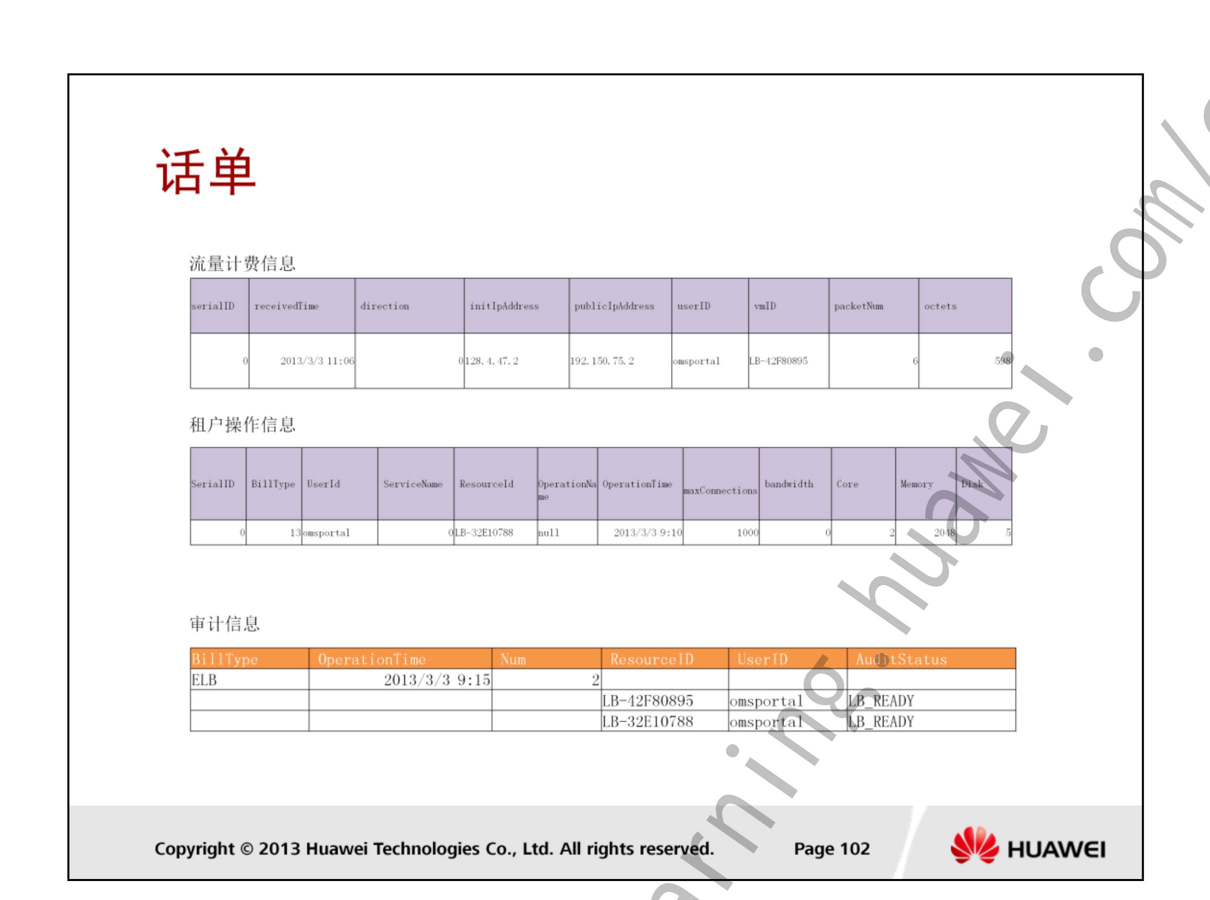
172.18.11.17

172.18.11.18

Page 101

HUAWEI

- 最小连接数：
  - ELB将用户的请求，转发到连接数最小的服务主机上
- 适用场景：
  - 适用于对响应时间和要求较高的场景



话单

流量计费信息

serialID	receivedTime	direction	initIpAddress	publicIpAddress	userID	vmID	packetNum	octets
0	2013/3/3 11:06	0	128. 4. 47. 2	192. 150. 75. 2	omsportal	LB-42F80895	6	598

租户操作信息

SerialID	BillType	UserId	ServiceName	ResourceId	OperationName	OperationTime	maxConnections	bandwidth	Core	Memory	Disk
0	13	omsportal	0	LB-32E10788	null	2013/3/3 9:10	1000	0	2	2048	5

审计信息

BillType	OperationTime	Num	ResourceID	UserID	AuditStatus
ELB	2013/3/3 9:15	2			
			LB-42F80895	omsportal	LB_READY
			LB-32E10788	omsportal	LB_READY

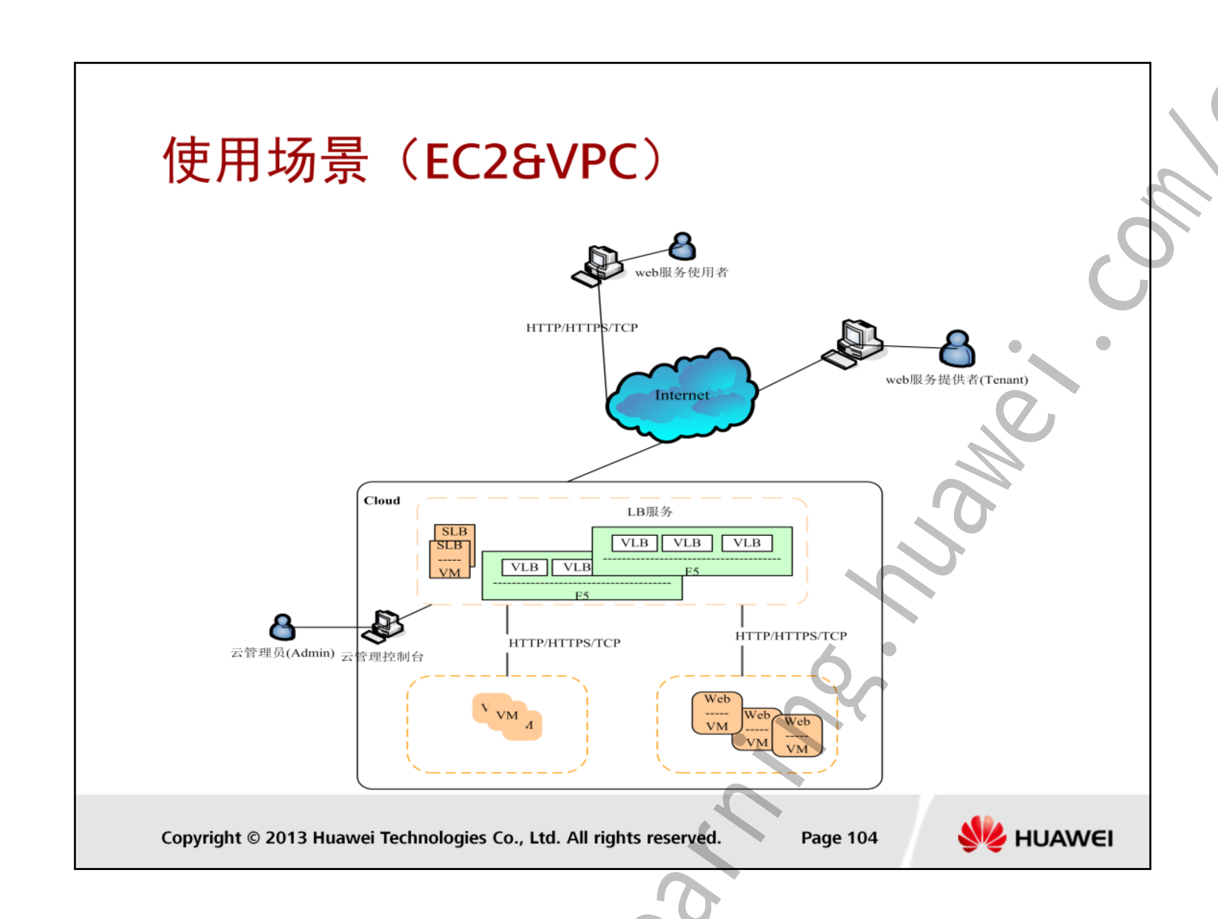
HUAWEI



目录

8. ELB





- **EC2 场景:**
  - **step1:** 租户申请多个EC2主机，并在其上部署同质化业务
  - **step2:** 租户申请ELB服务，并设置监听器、健康检查、会话保持、分发算法
  - **step3:** 租户将EC2主机关联到ELB上
- VPC场景:
  - **step1:** 租户申请VPC，并申请VPC主机，并在其上部署同质化业务
  - **step2:** 租户申请ELB服务，并设置监听器、健康检查、会话保持、分发算法
  - **step3:** 租户将VPC中的虚拟机主机关联到ELB上



目录

8. ELB



ELB服务开通配置（1）

FusionStack 系统管理
首页 系统管理 业务配置
配置项
服务和管理节点
系统LOGO
LB服务
LB-Manager管理
LB服务规格
LB虚拟机规格
管理子网配置
业务子网配置
LB服务申请限额
LB服务管理
添加
LB-Manager名称
LBM
1
添加LB-Manager
名称:
IP地址:
确定 取消

LB-Manager管理

LB-Manager为ELB服务的管理节点，管理ELB实例的配置、状态监控、告警。

- 添加ELB服务的管理节点，当前版本只支持添加一个管理节点
- 当前版本添加LB-Manager的，IP地址只能为ESC管理节点的浮动IP

ELB服务开通配置（2）

LB服务规格

定义Load balancing的服务规格模板，包括带宽、最大连接数、并发连接数。管理员可以定义不同的模板，满足不同场景的需求。

- 带宽用于限制ELB实例能够占用系统带宽的上限
- 最大连接数用于限制ELB所能支持转发连接数的上限

 Page 107 HUAWEI

ELB服务开通配置（3）

FusionStack 系统管理

首页 系统管理 业务配置

配置项
- 服务和管理节点
- 系统LOGO
- LB服务
  - LB-Manager管理
  - LB服务规格
  - LB虚拟机规格
  - 管理子网配置
  - 业务子网配置
  - LB服务申请限额
  - LB服务管理

添加 3

名称	LB服务规格
2U2G	

添加LB虚拟机规格
- 名称:
- LB服务规格:
- 镜像:
- CPU(个):
- 内存大小(MB):
- 磁盘大小(GB):

确定 取消

LB虚拟机规格

ELB实例的承载实体是一台虚拟机，该虚拟机上安装负载均衡软件，不同规格的虚拟机，提供不同的负载均衡能力，对应不同的LB服务规格。

- LB服务规格与LB虚拟机规格存在映射关系，这个关系由管理员定义
- CPU、内存、磁盘的规格与虚拟机相同

 Page 108 HUAWEI


ELB服务开通配置（4）
FusionStack
系统管理
首页
系统管理
业务配置
配置项
服务和管理节点
系统LOGO
LB服务
LB-Manager管理
LB服务规格
LB虚拟机规格
管理子网配置
业务子网配置
LB服务申请限额
LB服务管理
添加
名称
子网IP
4
管理&业务子网配置
ELB虚拟机有两个平面，管理平面和业务平面，管理子网用于ELB虚拟机管理地址的分配，业务子网用于转发面地址的分配。
每个站点都需要配置管理子网和业务子网
Vlan ID不能与系统中服务集群中的vlan资源冲突
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 109
HUAWEI

ELB服务开通配置（5）

FusionStack
系统管理
首页
系统管理
业务配置
配置项
服务和管理节点
系统LOGO
LB服务
LB-Manager管理
LB服务规格
LB虚拟机规格
管理子网配置
业务子网配置
LB服务申请限额
LB服务管理
设置
服务集群
TESTLB
配置LB服务申请限额
服务集群:
LB服务申请上限:
确定
取消
5

LB服务申请限额

系统中，ELB的实例资源需要设置上限，对每一个服务集群，设置ELB实例上限。

HUAWEI



目录





目录

9. EC2

 Page 112



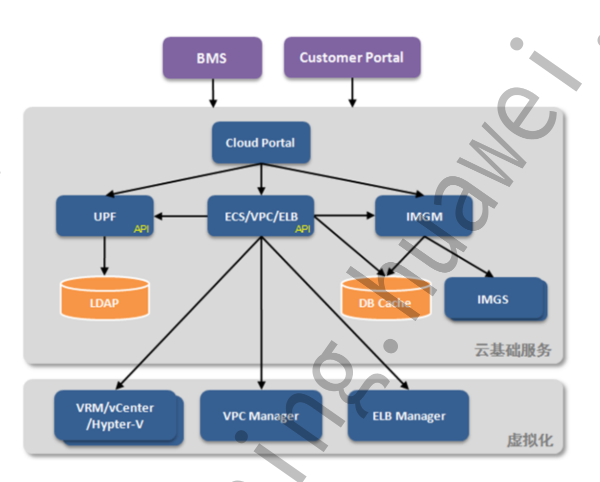
弹性计算

云基础服务基于华为虚拟化（FusionCompute）提供的基础虚拟化能力，向上提供包含弹性计算、VPC、ELB服务等。

弹性计算服务：提供对虚拟机实例、卷、安全组、弹性IP等虚拟资源的管理能力；

VPC服务：虚拟私有云，提供vFW、子网等管理能力；

ELB服务：向云租户（tenant）提供web服务的负载均衡能力（软件负载均衡）；



弹性计算 - 典型场景

市场定位
- ISP/ICP客户，尤其是中小型ISP/ICP
- 为用户提供Web应用托管平台

功能特性
- 弹性配置，按需租用：通过互联网直接租用计算、存储、网络等虚拟资源。
- 自助服务，快速部署：自助申请/调度资源、计费、查询，无需人工服务。
- 成本低，体验好：低于传统业务模式的TCO，自助服务提高响应速度

商业模式
- 利用中小ISP/ICP转售云平台服务
- 按资源使用付费
- 自助申请，自助付费

4 用户申请并使用虚拟服务器资源
2 用户通过互联网Web界面登陆Portal
网络资源池
存储资源池
计算资源池
云计算IDC
5 根据用户用量生成计费信息并扣费
1 通过云计算平台将物理资源整合成资源池
3 验证用户身份。（注册、鉴权）
鉴权系统
物理设备

 Page 114 HUAWEI

- ISP(Internet Service Provider)，互联网服务提供商，即向广大用户综合提供互联网接入业务、信息业务、和增值业务的电信运营商。ISP是经国家主管部门批准的正式运营企业，享受国家法律保护。
- **目前按照主营的业务划分，中国ISP主要有以下几类：**

1.搜索引擎ISP：到2005年底，使用过搜索引擎业务的互联网用户达89.1%。目前中国搜索引擎市场ISP，比如百度，提供的搜索服务也越来越丰富，包括地图搜索、论坛搜索、博客搜索等越来越多的细分服务。

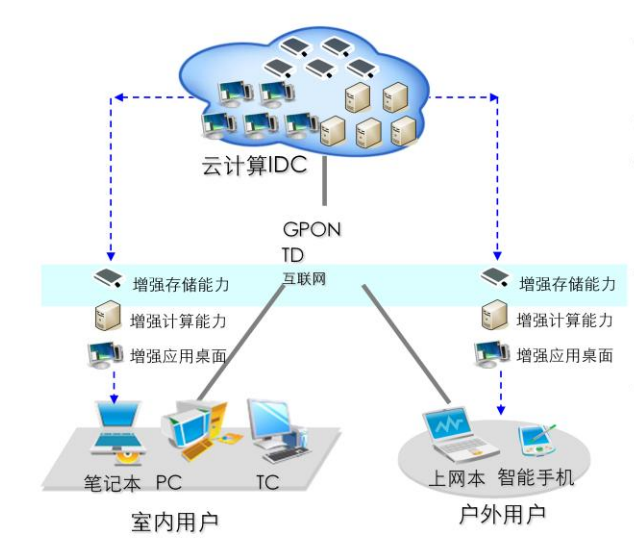
2.即时通信ISP：即时通信ISP主要提供基于互联网和基于移动互联网的即时通信业务。由于即时通信的ISP自己掌握用户资源，因此在即时通信的业务价值链中，即时通信ISP能起到主导作用。这在同运营商合作的商业模式中非常少见。

3.移动互联网业务ISP：移动互联网业务ICP主要提供移动互联网服务，包括：WAP上网服务、移动即时通信服务、信息下载服务等。

4.门户ISP提供新闻信息、文化信息等信息服务：门户ICP以向公众提供各种信息为主业，具有稳定的用户群。门户ICP的收入来源比较广，包括在线广告、移动业务、网络游戏及其他业务。比如：新浪、搜狐、网易和雅虎等门户网站（包括行业门户）。

- 网络内容服务商 英文为 Internet Content Provider 简写为ICP，即向广大用户综合提供互联网信息业务和增值业务的电信运营商。其必须具备的证书即为ICP证。

弹性计算 - 典型场景



- 对个人计算机的补充，弥补当前设备计算、存储、应用能力不足
- 上网本、宽带用户的增值业务
- 在线存储：通过GPON或宽带将用户数据存储到云计算IDC，并可通过多种终端设备访问
- 计算增强：使用云计算IDC中的高规格虚拟服务器处理大计算量应用（如照片处理、DV剪辑等）
- 虚拟桌面：使用瘦客户端（TC）等使用计算机应用，不需要购买额外的PC，低功耗免维护





目录

9. EC2

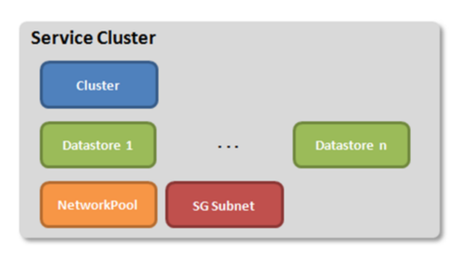


虚拟化站点与服务集群

弹性计算服务基于华为虚拟化提供基础虚拟化能力，向上提供虚拟机实例、卷、安全组、弹性IP等服务功能。

虚拟化站点是指一个独立的虚拟化管理节点，云基础服务在使用虚拟化资源前，需要先将站点的可用资源（集群、存储和网络资源等）添加到云基础服务。

服务集群被定义为一个包含计算、存储和网络资源的逻辑单元，是云基础服务对虚拟化站点资源的一种使用方式，可以看做是一个虚拟资源池。





- 华为虚拟化支持多个站点的级联，级联后可通过主级联控制器直接访问其他站点。为了更灵活的支持级联场景下虚拟化站点的接入，云基础服务引入了“虚拟化接入点”的概念。单独的虚拟化站点可以看做是一个虚拟化接入点，级联在一起的多个虚拟化站点也可以看做是一个虚拟机接入点，其区别在于经过级联的虚拟化接入点中同时存在多个站点。

- 从使用上来讲，虚拟化站点是否级联并不影响云基础服务对虚拟化资源的使用。
- 一个服务集群包含一个虚拟化站点中的逻辑集群（计算资源）、该逻辑集群下可以使用的数据存储、以及网络池和安全组子网。其中网络池中配置了虚拟化提供的DVS和Vlan资源，为VPC、兼容VPC、Vlan等业务提供网络资源，安全组子网主要为安全组业务提供网络资源。

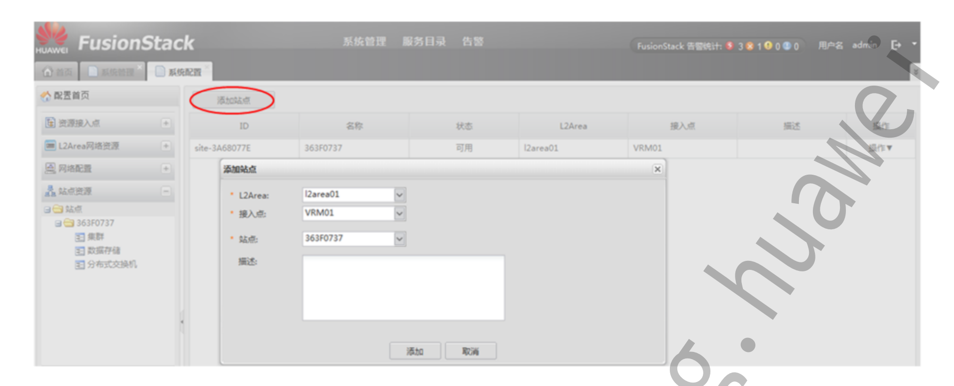


- 云基础服务支持多个接入虚拟化站点。

虚拟化站点管理

2、添加虚拟化站点

添加站点前需要先创建L2Area（L2Area相关概念请参见VPC特性介绍）。



 Page 119




服务集群管理
1、添加服务集群
FusionStack
系统管理
服务目录
告警
admin
基本信息
选择集群
选择数据存储
配置网络池
配置安全组子网
确认信息
输入服务集群的基本信息.
名称:
描述:
下一步
取消
2、修改服务集群
服务集群支持数据存储资源和网络资源的动态扩容和减容。
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 120
HUAWEI

虚拟化站点与服务集群

约束和限制

1、添加到服务集群数据存储资源应该为共享类型，即该服务集群所关联的虚拟化站点中的逻辑集群下的计算节点均可访问这些数据存储，以满足用户卷的自由挂卸载。云基础服务并不强制要求数据存储为共享类型，在某些场景，如不提供用户卷和虚拟机快照业务时，可以选择本地磁盘类型的数据存储。

2、从云基础的模型上看，服务集群是与站点的逻辑集群一一对应的，因此要求计算、存储和网络资源在系统规划时以站点的逻辑集群为单位，必须避免虚拟化资源同时被多个逻辑集群同时使用，如数据存储和分布式交换机（DVS）应该仅在某一个集群下可见。

3、云基础服务的VPC、兼容VPC及安全组均依赖于虚拟化的Vlan资源，要求虚拟化站点的一个逻辑集群对应有一个分布式交换机，该分布式交换机覆盖该逻辑集群下的所有站点。





目录

9. EC2





- 镜像是用于创建虚拟机的原始文件。受限于虚拟化支持的镜像类型，云基础服务仅支持VHD格式的镜像文件。在部署形态上，镜像服务器是一台独立、用于存储镜像文件的服务器，另外，镜像服务器以NFS协议向虚拟化提供镜像下载的能力。
- 价值特性

1、支持多台镜像服务器，同时同一镜像可存储于不同的服务器，进行负荷分担；

2、镜像服务器支持多路径存储，提供单台镜像服务器存储空间的扩减容能力；

镜像与镜像服务器

镜像管理

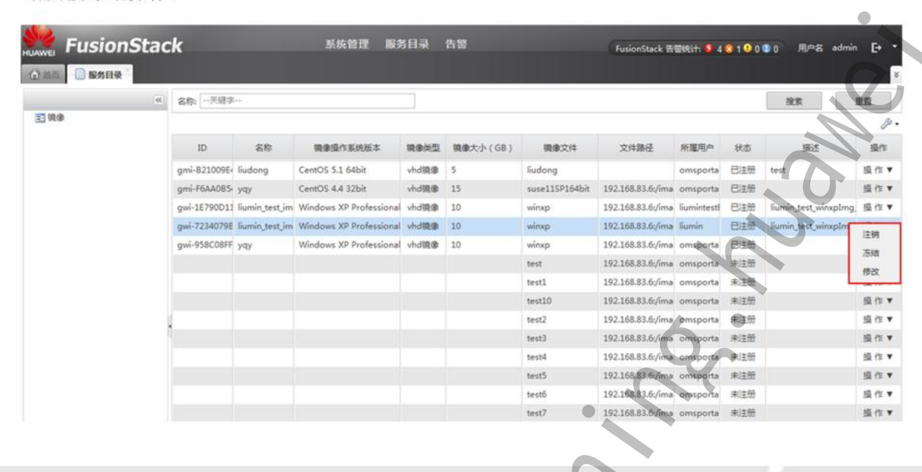
1、镜像制作

镜像利用虚拟化站点的模板导出功能，将安装和配置（软件或其他系统配置等）完成的虚拟机模板导出VHD文件到镜像服务器。

镜像与镜像服务器

2、注册镜像

系统支持自动扫描镜像服务器上的镜像文件，可通过云基础服务Portal注册、注销、删除、冻结及接冻结操作。

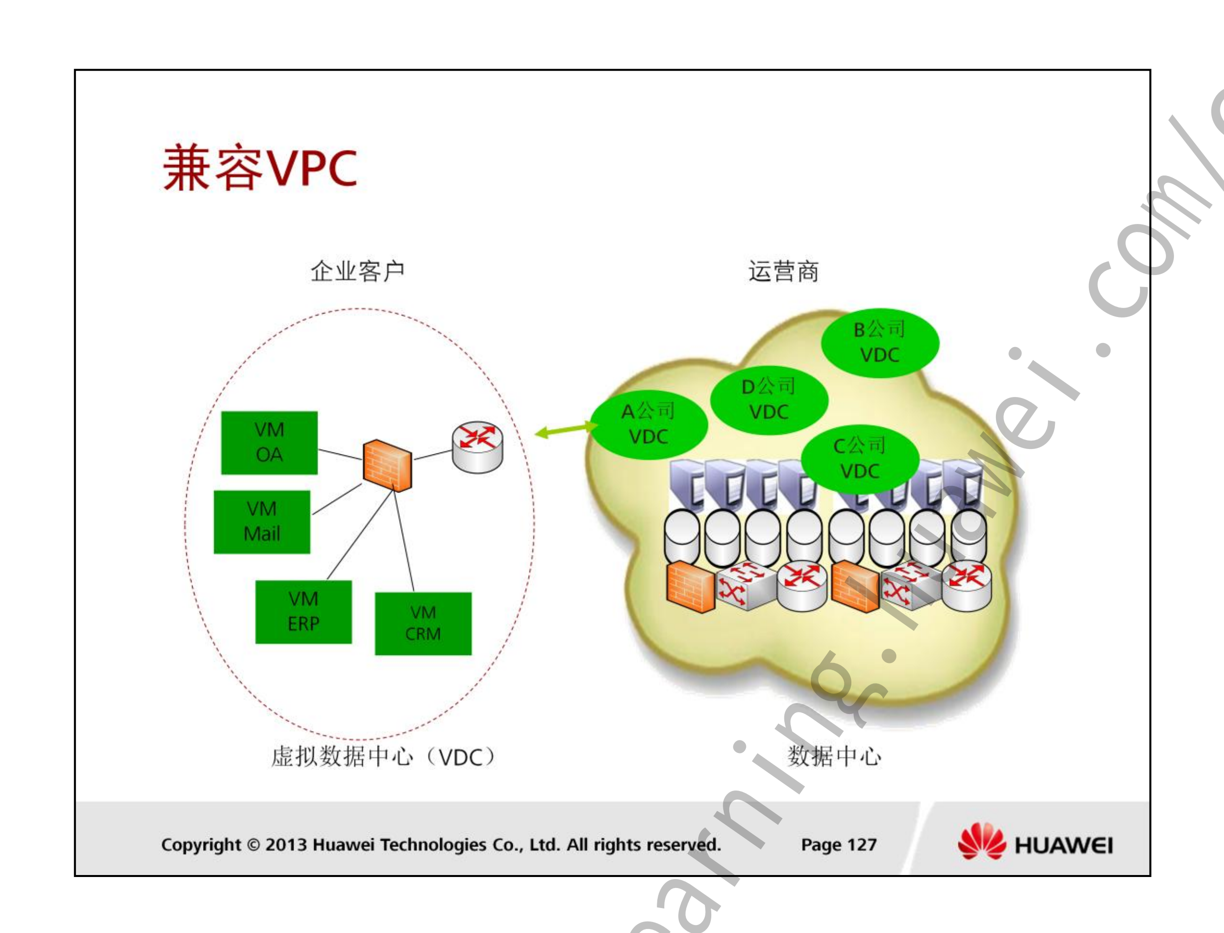




目录

9. EC2

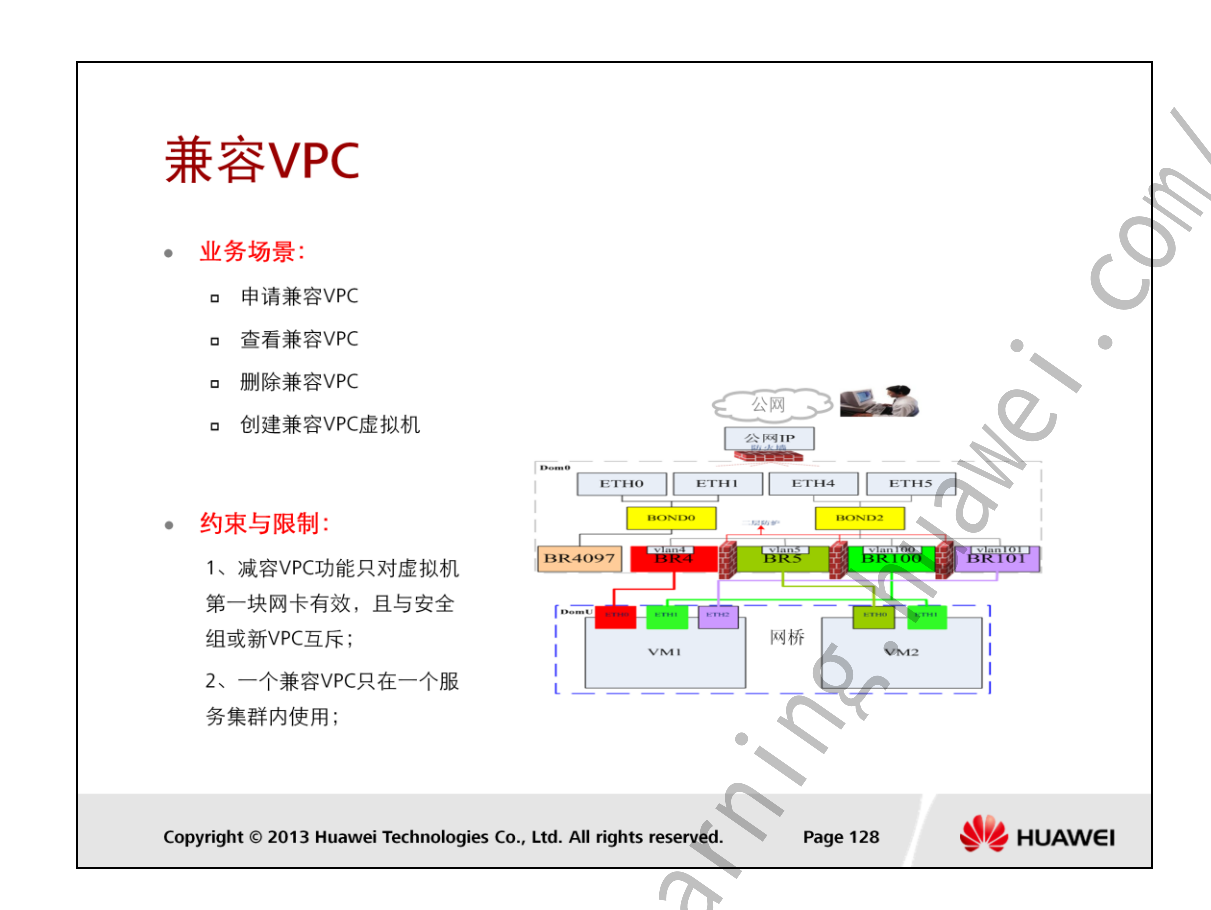




- **定义：** VPC（Virtual Private Cloud）虚拟私有云，实现数据中心基础上的局域网功能，一个VPC相当于一个局域网。
- **特性描述：**

  虚拟私有云是一种面向企业的云应用。企业可以在公有云平台上申请虚拟私有云。在虚拟私有云中，企业具有完全独立的IP地址空间设置，以及与其他不在该私有云中的虚拟机的完全网络隔离。这种隔离是完全的二层隔离。

  企业用户可以使用VPN网关将这个虚拟私有云和自己企业的网络连通，然后像使用自己的IT设施一样使用虚拟私有云中的虚拟机。



- 兼容VPC使用VLAN实现。在计算节点行上，一个VLAN对应一个软件网桥。接入交换机上，所有端口默认开放所有的VLAN。汇聚交换机上，到不同站点的接入交换机的端口仅开放该站点的VLAN。经过云基础服务层的封装，VLAN资源被限定在一个服务集群内使用，因此用户所创建的兼容VPC不支持跨服务集群，只能在一个服务集群中使用。

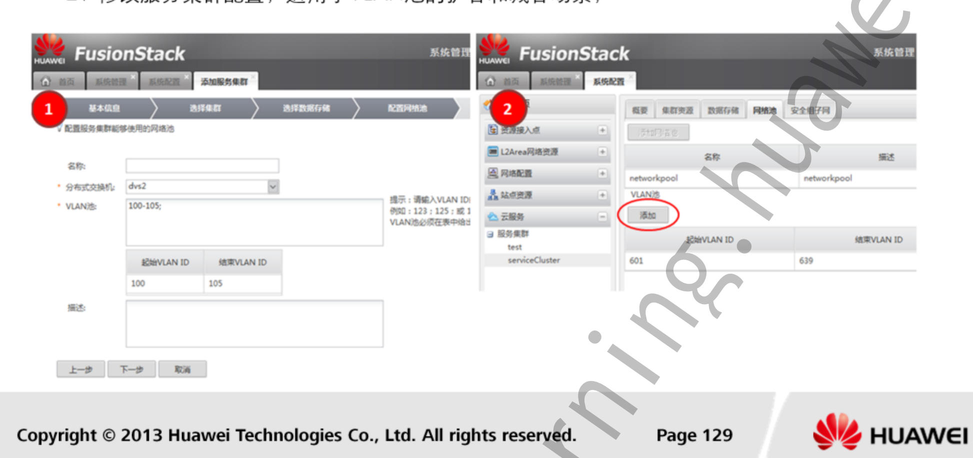
兼容VPC

兼容VPC的相关配置

兼容VPC所使用的VLAN资源需要在虚拟化站点上提前规划，以集群为单位创建好对应的分布式交换机，并在云基础服务Portal上进行配置，可通过两种方式进行配置：

1、创建服务集群的配置网络池过程中，配置该服务集群下可使用的DVS及VLAN池；

2、修改服务集群配置，适用于VLAN池的扩容和减容场景；



 Page 129 HUAWEI

- DVS，Distributed Virtual Switch，分布式虚拟交换机。



目录

9. EC2



多虚拟网卡

多虚拟网卡应用场景：

- 由于虚拟机上会部署不同的业务，要求虚拟机有多个虚拟网卡，每个网卡配置不同网段的IP地址。
- 虚拟机每个网卡具有不同的MAC地址，可以将网卡划分到不同的VLAN，配置网卡IP地址及路由。

功能说明：

创建虚拟机的时候，能指定多个虚拟网卡，以及每个虚拟网卡的相关属性，满足一些对虚拟机有多网卡要求的场景。创建多网卡的虚拟机后，实际上每个虚拟网卡属于一个VLAN，除第一个网卡由系统分配IP外（VPC除外），其余的网卡IP由用户登陆虚拟机自己手动配置。

业务场景：

- 创建多网卡虚拟机
- 虚拟机添加/删除虚拟网卡

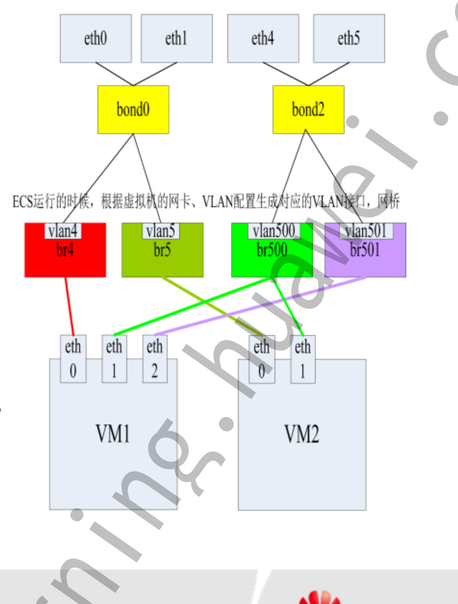
 Page 131



多虚拟网卡

在CNA上，一个VLAN就是一个软件网桥，同一个VLAN上的网卡挂在同一个网桥上，所以能够节点内自交换。接入交换机上，默认放开所有的VLAN。汇聚交换机上，到每个集群的几个网口上放开这个集群的VLAN。这里和兼容VPC是一样的，因为使用的是相同的技术。右图只是以绑定为例进行说明，实际使用中也可以不进行绑定，VLAN可以直接创建在eth口上。虚拟机的eth0为受控的网卡，安全组、给虚拟机分配地址都是在该网卡上生效。

其他网卡在创建虚拟机时需要指定其所属的VLAN（如vlan500，vlan501，此VLAN需要用户事先申请）。CNA根据VLAN和CNA上的接口对应关系在主机上创建VLAN和网桥。





多虚拟网卡

限制与约束

1、用户只能增删多网卡，而不能删除或者添加基本网卡

2、一个虚拟机可以配置的多网卡数量最多为7个(即一台虚拟机最多支持8块虚拟网卡)

3、用户在新增多网卡时，必须指定VLAN或新VPC的子网

4、虚拟机第一块网卡外的其他网卡的VLAN与虚拟机必须在同一个AvailabilityZone中

5、本特性依赖于多VLAN特性和VPC特性



多虚拟网卡

扩展内容

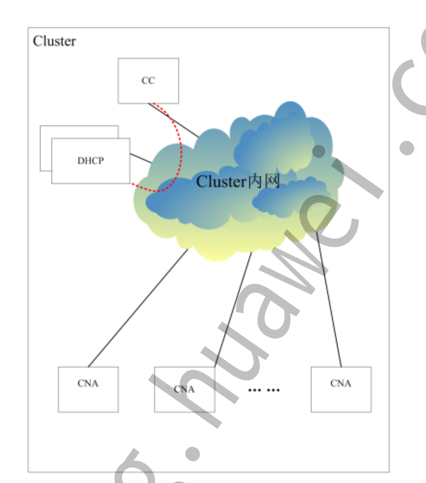
1、虚拟机多网卡的IP如何配置?

虚拟机用户通过第一块网卡登录虚拟机，

配置其他网卡IP地址

2、虚拟机基本网卡IP地址如何分配和获取?

每个Cluster内有一对DHCP，专门为VM分配IP地址。



- DHCP受控情况 - DHCP由CRM控制
- 虚拟机基本网卡使用IP地址和VLAN，
- 由CRM指定，这种模式下才能支持安全组。
- DHCP不受控 - DHCP不受CRM控制
- CRM不会给虚拟机分配私有IP地址。
- 业务面的DHCP配置全部由人工保证和完成，虚拟机通过该DHCP动态获取地址



 Page 134 HUAWEI



目录

9. EC2

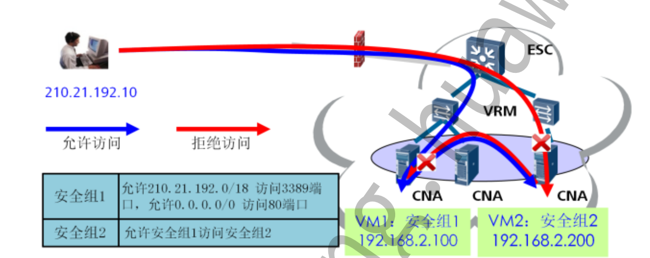


虚拟机支持安全组

- 每个虚拟机提供一个VLAN太奢侈，因为VLAN只有4096个。所以需要提供一些容量较小的容器，并可以灵活配置互访关系，用于部署不同的应用。
- 网络安全组为虚拟机定义防火墙规则，这些规则确定哪些网络流量可以进入虚拟机，同时防护墙规则可以动态添加到安全组中，为正在运行中的虚拟机或将来启动的虚拟机增强安全性。对于安全组的访问限制功能，主要通过iptables实现。
- 该功能为用户提供安全、可靠的隔离策略，确保只有授权的访问才被接受。

业务场景：

- 创建安全组
- 增加安全组规则
- 删除安全组规则
- 创建安全组虚拟机
- 释放安全组
- 从安全组分配私有IP地址





虚拟机支持安全组

安全组配置

用户所创建的安全组是在服务集群的范畴内的，而服务集群与站点的逻辑集群是一一对应的，因此要使得某个服务集群提供安全组业务，需要以站点的集群为单位进行规划，确定用于安全组特性的网段和对应的VLAN，并在对应的接入和汇聚交换机上完成网关、 VLAN通过的相应端口等相应配置。

在云基础服务Portal上，根据业务需要可为服务集群配置安全组子网，配置完成后，该服务集群即可提供安全组业务。另外，安全子网依赖于网络池的配置。



HUAWEI

虚拟机支持安全组

安全组特性详解：

1、安全组大小支持1~128；

2、属于同一个安全组的VM，默认全部互联互通；属于不同安全组的虚拟机，默认隔离。

3、安全组规则分为两种：

组间授权：允许哪些安全组访问本安全组。

IP授权：允许哪些对端网络设备访问本虚拟机。可以配置允许的对端IP地址段、端口号段和规则协议。

4、规则协议支持TCP、UDP和ICMP

5、创建一个安全组，系统在可用的安全组子网中划分出一个网段。划分时，系统会将配置的安全组子网的网段（如 “192.168.1.0/24” ）的第一个和最后一个IP去掉（网关地址和广播地址）。



虚拟机支持安全组

约束和限制：

1、一个虚拟机不能同时属于两个安全组；

2、不支持安全组大小动态扩大或缩小；

3、虚拟机不支持更换安全组；

4、虚拟机的非主网卡不支持加入安全组；

5、安全组不支持跨集群；

6、安全组的规则是基于内部IP地址实现的。即当安全组规则生效时，只允许对端访问本端的内部IP地址，如果要允许对端访问本端的公共IP或弹性IP地址，需要另行添加规则；

7、只有安全组内所有的虚拟机都删除后，才允许删除安全组；

8、安全组规则随虚拟机的启动而自动生效，虚拟机迁移，HA不影响安全组规则；
虚拟机启动后，如果修改其安全组规则，修改后的规则对已启动的虚拟机生效。

9、安全组规则是单向授权。例如：A安全组可以访问B安全组，不表示B安全组可以访问A安全组。

10、一个安全组可最多包含30条规则。



虚拟机支持安全组

扩展内容：

1.安全组的虚拟机的IP是怎么分配的?

安全组虚拟机第一块网卡的IP地址是由VRM上自带的DHCP自动分配的

2.安全组的虚拟机怎样连接公网?

当虚拟机需要与公网互通时，分配公共IP；当虚拟机上的业务需要与公网互通并且业务访问地址固定不变时，虚拟机创建时申请弹性IP。

3.兼容VPC和多网卡为什么不能使用安全组?

安全组是和IP段绑定的，IP段是和VLAN段绑定的，虚拟机网卡和VLAN绑定。默认路由只有一条，安全组没有必要针对其他的网卡。基本网卡用来做通用通信用，扩展网卡只用来和内部同VLAN的虚拟机网卡通信，这个VLAN都是一个用户申请的，不需要安全组。

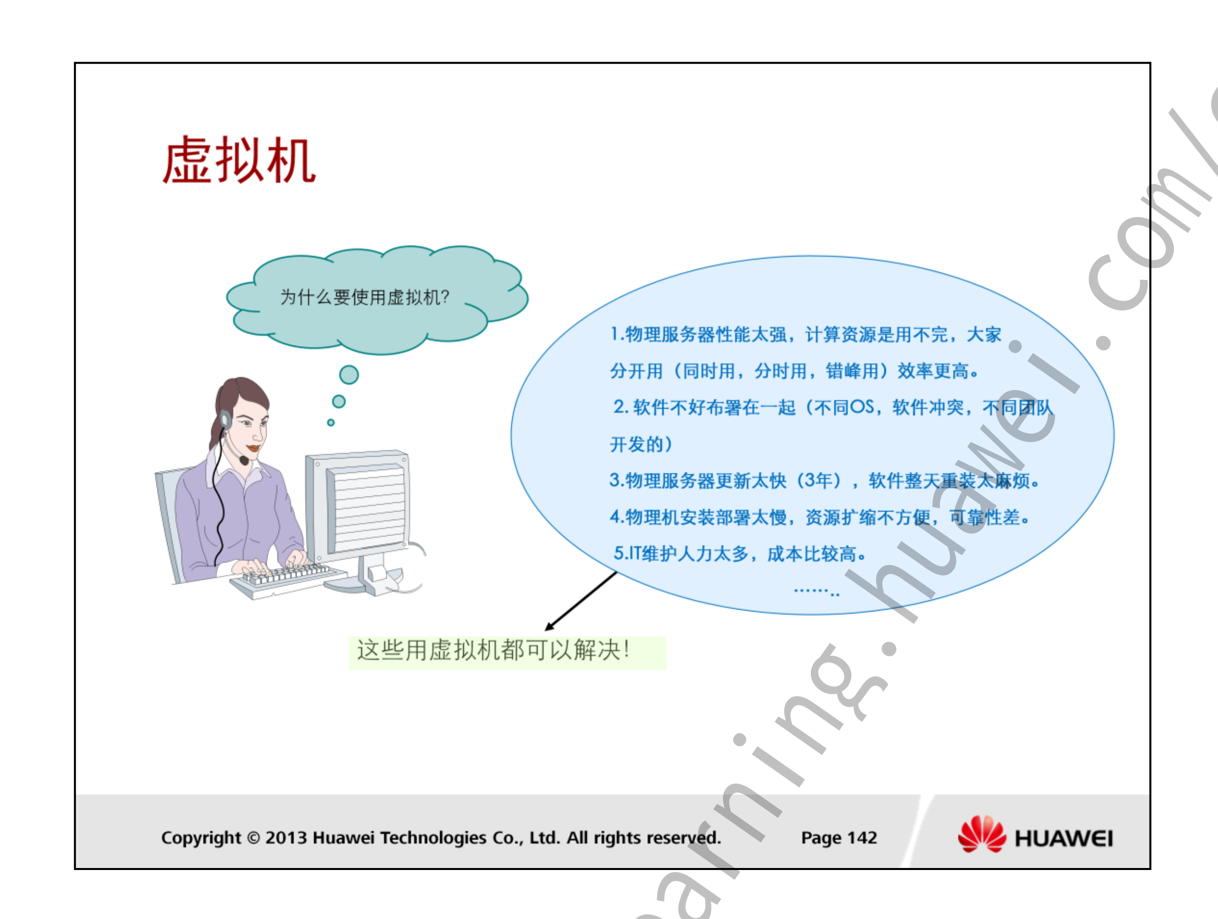




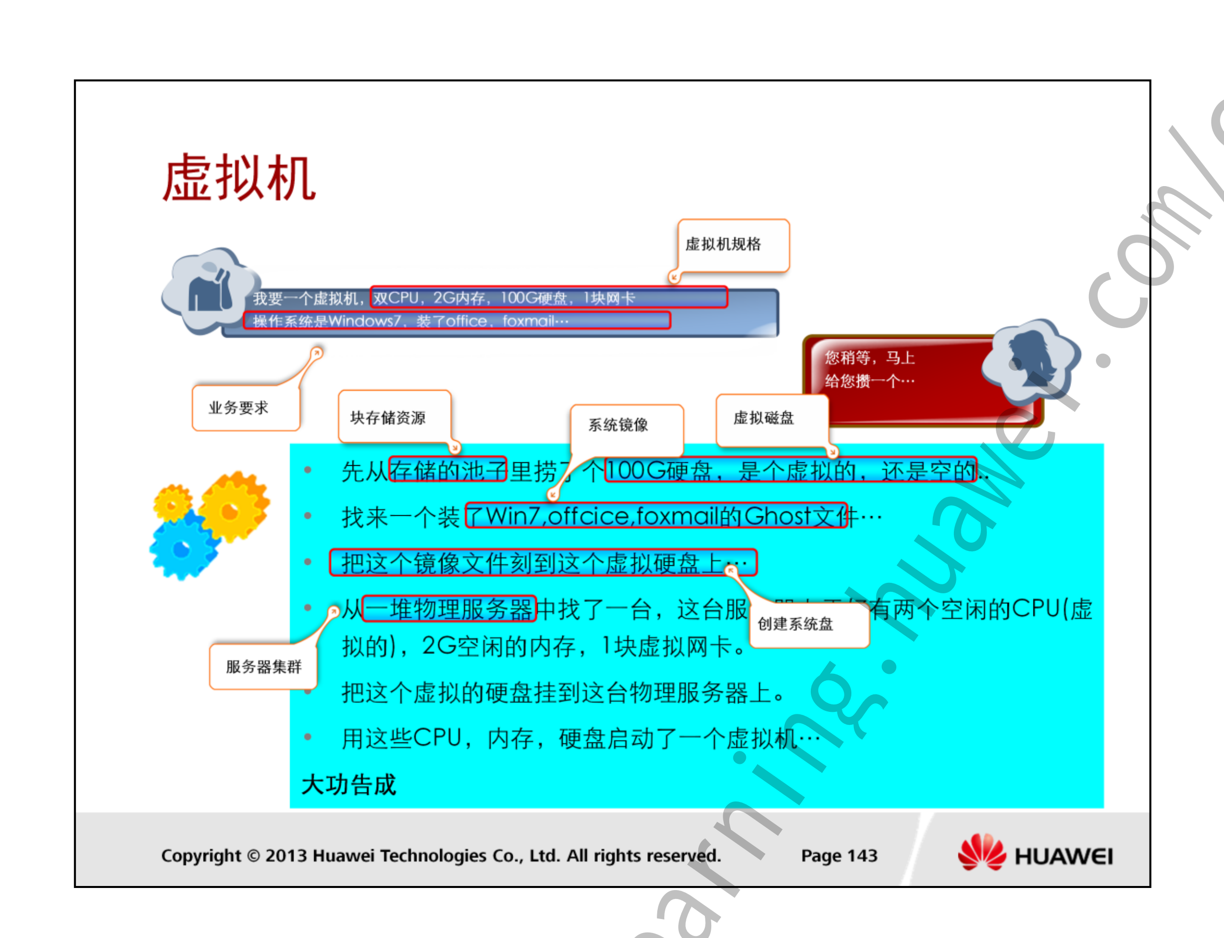
目录

9. EC2





- 虚拟机依赖于虚拟化技术，虚拟化是指计算机元件在虚拟的基础上而不是真实的基础上运行。虚拟化技术可以扩大硬件的容量，简化软件的重新配置过程。CPU的虚拟化技术可以单CPU模拟多CPU并行，允许一个平台同时运行多个操作系统，并且应用程序都可以在相互独立的空间内运行而互不影响，从而显著提高计算机的工作效率。


虚拟机
虚拟机规格
我要一个虚拟机，双CPU，2G内存，100G硬盘，1块网卡
操作系统是Windows7，装了office，foxmail…
您稍等，马上给您攒一个…
业务要求
块存储资源
系统镜像
虚拟磁盘
先从存储的池子里捞了一个100G硬盘，是个虚拟的，还是空的…
找来一个装了Win7,offcice,foxmail的Ghost文件…
把这个镜像文件刻到这个虚拟硬盘上…
从一堆物理服务器中找了一台，这台服务器上正好有两个空闲的CPU(虚拟的)，2G空闲的内存，1块虚拟网卡。
创建系统盘
服务器集群
把这个虚拟的硬盘挂到这台物理服务器上。
用这些CPU，内存，硬盘启动了一个虚拟机…
大功告成
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 143
HUAWEI

虚拟机 - 创建虚拟机

No.	参数	说明	No.	参数	说明
1	镜像ID	注册镜像后系统生成的唯一标识镜像的ID（条件可选，无系统盘虚拟机不需要镜像）	8	密钥对	用于SSH免密码登陆，仅支持Linux
2	数量	创建虚拟机的数量，支持批量创建同质虚拟机（必选）	9	主网卡限速	虚拟机主网卡的上限速度
3	规格	创建的用户规格ID，标识了虚拟机的CPU、内存、系统盘，以及QoS参数等（必选）	10	多网卡	支持最多7个虚拟网卡（不含主网卡），可为每个虚拟网卡设置限速、所在Vlan或子网
4	是否HA	是否自动恢复故障虚拟机（必选）	11	别名	自定义虚拟机别名，标识不同虚拟机
5	安全组	虚拟机要加入的安全组名称（条件可选，和VPC、兼容VPC三选一）	12	虚拟机密码	自定义虚拟机初始密码
6	VPC	VPC子网ID（VPC详细请参见VPC特性培训胶片）（条件可选）	13	虚拟机类型	支持创建无系统盘虚拟机，默认为有系统盘
7	兼容VPC	虚拟机要加入的兼容VPC的ID（条件可选）	14	时钟同步模式	支持自由时钟和同步时钟（与系统时钟同步）两种模式



- 云基础服务暂未提供用户界面来完成虚拟机等业务的操作，从接口来讲，创建虚拟机需要：

1、创建虚拟机需要的镜像已经被注册，系统为该镜像分配了镜像ID（无系统盘虚拟机不需要镜像）；

2、已经在系统中创建了虚拟机规格；

3、已经在系统中创建了虚拟机所属的安全组、VPC或兼容VPC的网络对象；

虚拟机 - 其他业务场景

除了创建虚拟机，还支持以下对虚拟机的操作和业务场景：

1、删除虚拟机：释放虚拟机所占用的计算和存储资源（仅释放系统盘占用的存储资源，用户盘仅卸载），删除虚拟机的所有网卡。

2、查询虚拟机：支持按照zone、私有IP地址过滤查询，支持查询虚拟机初始设置的操作系统密码。

3、停止虚拟机：支持安全停止和强制停止。

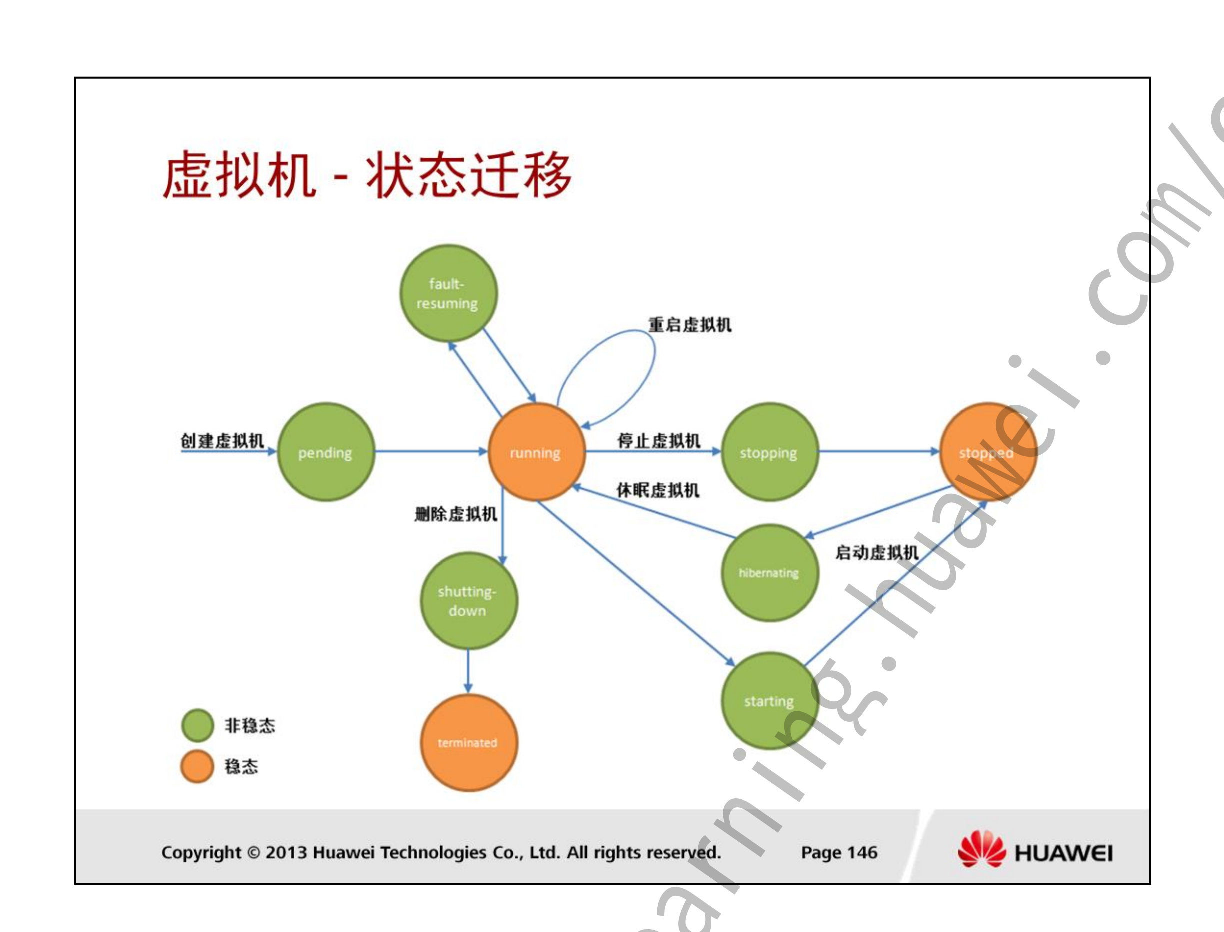
4、重启虚拟机：支持安全重启和强制重启。

5、休眠虚拟机

6、启动虚拟机

7、修改虚拟机属性：支持修改虚拟机规格（CPU、内存及QoS参数）、虚拟机网卡限速、虚拟机非主网卡所在VLAN、虚拟机别名、虚拟机启动方式等。




虚拟机 - 状态迁移
fault-
resuming
重启虚拟机
创建虚拟机
pending
running
停止虚拟机
stopping
stopped
休眠虚拟机
删除虚拟机
hibernating
启动虚拟机
shutting-
down
starting
terminated
非稳态
稳态
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 146
HUAWEI



目录

9. EC2



用户卷

用户卷是为用户提供的除了系统磁盘之外的存储空间，支持AvailabilityZone范围内的自由挂卸载。向用户提供弹性存储空间能力，用户可通过挂载和卸载用户卷实现虚拟机之间的数据共享，满足各种业务需求。

支持的操作：

1、创建用户卷：指定要创建的用户卷大小，以及AvailabilityZone进行创建创建。支持创建共享卷（共享卷可同时挂载至多个虚拟机上），支持瘦分配。

2、删除用户卷

3、查询用户卷：可查询用户卷的状态（创建状态及挂载状态），类型及创建时间等。

4、卸载用户卷：从虚拟机卸载用户卷，支持卸载系统卷。

5、挂载用户卷：将创建成功或从其他虚拟机上卸载下来的卷挂载至虚拟机上。支持虚拟机系统卷的挂载（从VM1上卸载，挂载至VM2上，满足特殊场景需求），同时系统卷也可作为用户卷挂载，作为数据磁盘来使用。



用户卷

相关配置

和虚拟机的系统磁盘相同，用户卷依赖于虚拟化站点提供的数据存储能力，云基础要求配置在服务集群中的数据存储必须能够在该服务集群对应的站点的逻辑集群中共享。



- **约束和限制：**

1、瘦分配类型卷最大支持2TB，非瘦分配类型卷最大可支持30TB

2、一个虚拟机最大支持挂载10块用户卷，共享卷同时所挂载到虚拟机的数量不能超过4个；

3、不支持在线卸载卷（即虚拟机状态必须在stopped时才可以卸载）。



目录

9. EC2



弹性IP & 网络端口地址转换（NAPT）

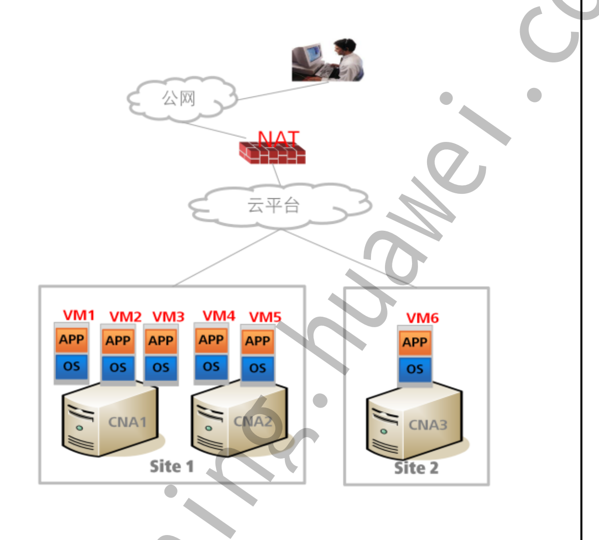
弹性IP价值

允许外部用户使用固定的公网地址访问某台虚拟机。

弹性IP功能描述

通过在对外连接的防火墙上设置NAT参数，可以将公网地址映射到某个虚拟机的私网地址之上。

在一个数据中心中，允许虚拟机使用的公网地址是有限的，并且也不是每个虚拟机都需要公网地址，所以系统分配的虚拟机默认不分配永久公网地址。当用户需要在虚拟机上对公网提供业务的话，需要申请弹性IP地址。当用户申请弹性IP地址并绑定到某台虚拟机后，云管理系统将自动在防火墙上为该虚拟机配置NAT映射。用户可以修改解除弹性IP与虚拟机的绑定关系，还可以释放这个弹性IP地址。

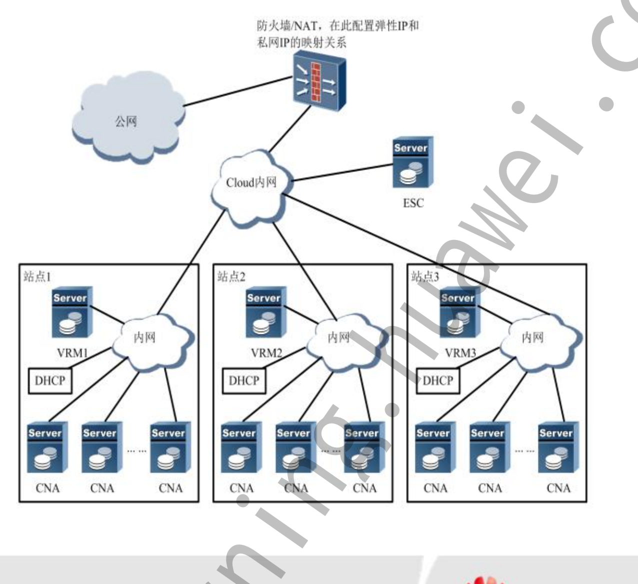




弹性IP & 网络端口地址转换（NAPT）

- 弹性IP由用户申请，由网络管理员将申请到的外网IP配置为弹性IP，用户绑定弹性
- IP与虚拟机后，可在Internet上通过弹性IP访问虚拟机。并且将此弹性IP绑定到其他虚拟机，实现手动的浮动IP的功能。
- 公共IP，以及弹性IP和私有IP的映射

  都在该NAT设备上实现
- 云基础服务 配置弹性IP和公共IP地址池，以及控制的NAT设备地址支持多个虚拟网卡





HUAWEI

弹性IP & 网络端口地址转换（NAPT）

弹性IP与公共IP的区别

- 弹性IP也是公网的IP，公共IP也是公网的IP（这里公网和内网是相对而言的）。弹性IP与公共IP的区别是，弹性IP需要用户申请，公共IP由系统自动分配。
- 如果系统默认配置为运行虚拟机的时候即为虚拟机分配公共IP，则系统会为虚拟机分配一个公共IP，由于该IP是与虚拟机绑定的，用户对该IP没有所有权和操作权限。当虚拟机被关联到其他的弹性IP上，或者虚拟机被停止后，该IP就会被系统回收。
- 而弹性IP需要用户显示的执行释放操作后，系统才回收。一个公共IP或者弹性IP，只能绑定到一个私有IP。且一个私有IP也只能绑定到一个公共IP或弹性IP。



弹性IP & 网络端口地址转换（NAPT）

什么是NAPT?

- 网口地址转换（NAPT）功能，通过将虚拟机内部IP地址加内部端口映射为公网IP地址加外部端口，使多个虚拟机可以共享同一个公网IP和外部交互。
- 虚拟机内部IP地址加内部端口和公网IP地址加外部端口的映射在防火墙/NAT上实现，数据从公网进内网时，会进行数据包目的IP端口对的替换，将公网IP端口对替换为虚拟机内网IP端口对；数据从内网出公网时，会进行源IP端口对的替换，将虚拟机内网IP端口对替换成公网IP端口对。

NAPT和弹性IP的共同点及差别，有了弹性IP，为什么还需要NAPT?

- NAPT和弹性IP都需要提前规划并配置好公网IP地址池。
- 弹性IP和NAPT都可以使虚拟机和公网互通，但使用弹性IP的方式占用的公网IP多，每个申请弹性IP的虚拟机必须要占一个公网IP，而NAPT通过公网IP加端口映射的方法，使得一个公网IP可以映射到系统内部一个局域网，而不仅是一个虚拟机。
- NAPT IP和虚拟机映射时，可以将RDP、SSH、TELNET等不同的网络访问协议映射到不同端口上，用户还可以自定义协议和端口的映射关系。而弹性IP和虚拟机绑定时，不能做到网络访问协议和端口的自定义映射。

 Page 154



弹性IP & 网络端口地址转换（NAPT）

相关配置

系统规划之初，若要提供弹性IP特性和NAPT特性，需要规划用来分配的弹性IP地址范围和NAPT的端口映射绑定范围。





弹性IP & 网络端口地址转换（NAPT）

限制与约束

1、只有状态为运行中的虚拟机才可以关联弹性IP和NAPT；

2、只有安全组和VPC虚拟机可以使用弹性IP和NAPT功能，兼容VPC的虚拟机不能使用；

3、系统规划之初，若要提供弹性IP和NAPT功能，需要规划用来分配的弹性IP和NAPT IP地址范围；

扩展内容

1、只有安全组的虚拟机可以使用弹性IP和NAPT，兼容VPC和多VLAN不行？

因为没有给这些VLAN配网关和路由。如果配了路由，将公网IP指向NAT即可。

2、为什么两台绑定了弹性IP和NAPT功能的虚拟机互访还需要过外网？

路由如此，安全要求





目录

9. EC2

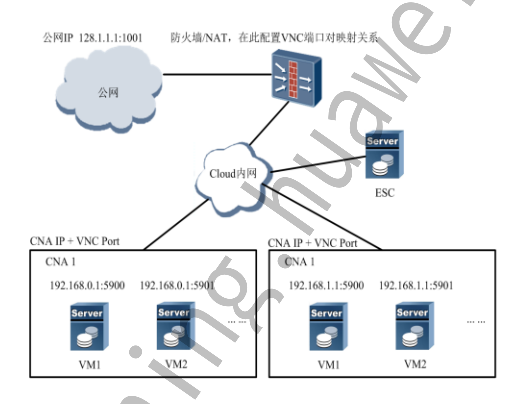


VNC登录

VNC协议是一种远程桌面登陆协议。 VNC（Virtual Network Computing），在虚拟机可用，网络正常，可以用RDP/ICA，ssh, telnet, ftp等方式从外网访问虚拟机。当虚拟机发生故障无法启动时，用户无法通过外部网络访问虚拟机，此时操作维护人员可以通过VNC连接到故障的虚拟机进行修复。

系统每创建一个虚拟机，计算节点CNA自动为虚拟机分配一个VNC端口，通过内网，可以直接通过VNC客户端登陆到虚拟机。

VNC特性提供的是通过公网的IP地址远程登陆虚拟机的一种方式。通过防火墙的NAT功能实现，本质上与NAPT特性相同。





VNC登录

限制与约束

1、IT管理员用于VNC连接登录虚拟机的外部IP与弹性IP、公共IP不能冲突

2、虚拟机必须在运行（Running）状态下才允许做端口映射。

3、VNC暴露给用户是不安全的，因此NAT上的VNC端口映射断开后，由用户重新发起连接请求。

4、从安全角度考虑，VNC连接时长默认为1小时。

5、VNC的连接速度很慢，局域网内的使用感受已经很差。提供外网连接用户体验会很差。

6、更新配置时，维护管理人员在确保ESC节点与NAT设备连接正常。

7、维护管理人员必须确保NAT设备的配置正确。

8、更新配置时，不允许有新的VNC申请，删除和查询操作。



VNC登录

扩展内容

1、为什么有定时断开VNC连接的时长的限制?

VNC暴露给用户是不安全的，目前ECS定时清除NAT上的VNC连接以增强安全性。因此NAT上的VNC端口映射断开后，由用户重新发起连接请求。

VNC并非是安全的协议，虽然VNC伺服程序需设置密码才可接受外来连接，且VNC客户端与VNC伺服程序之间的密码传输经过加密，但仍可被轻易的拦截到并使用暴力搜索法破解。后续版本中，VNC连接可以使用SSL加密传输，以增强传输的安全性。

2、为什么VM迁移后VNC连接会中断?

因为虚拟机在热迁移处理过程中VNC port会变化，所以需要手动重新建立VNC连接。





目录



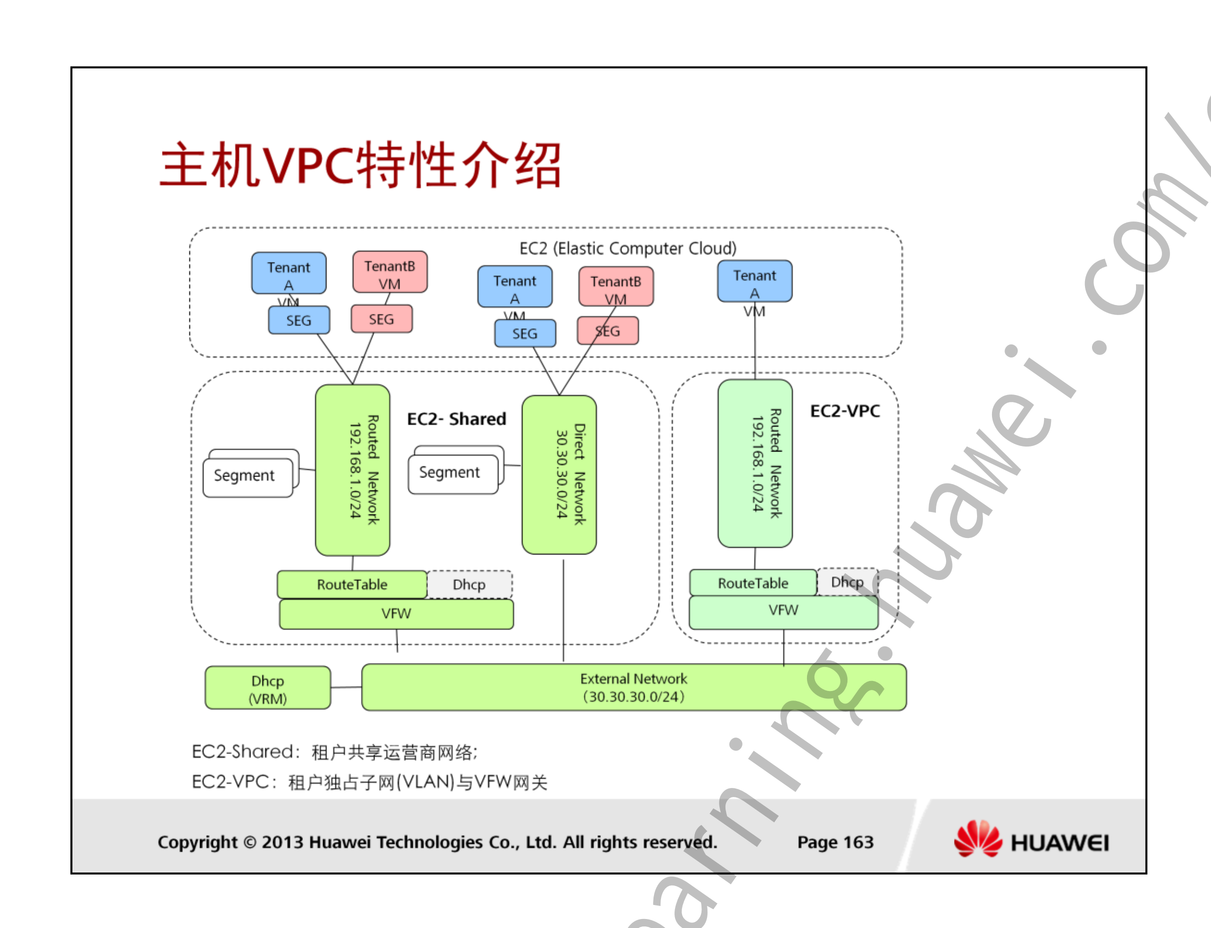




目录

10. VPC





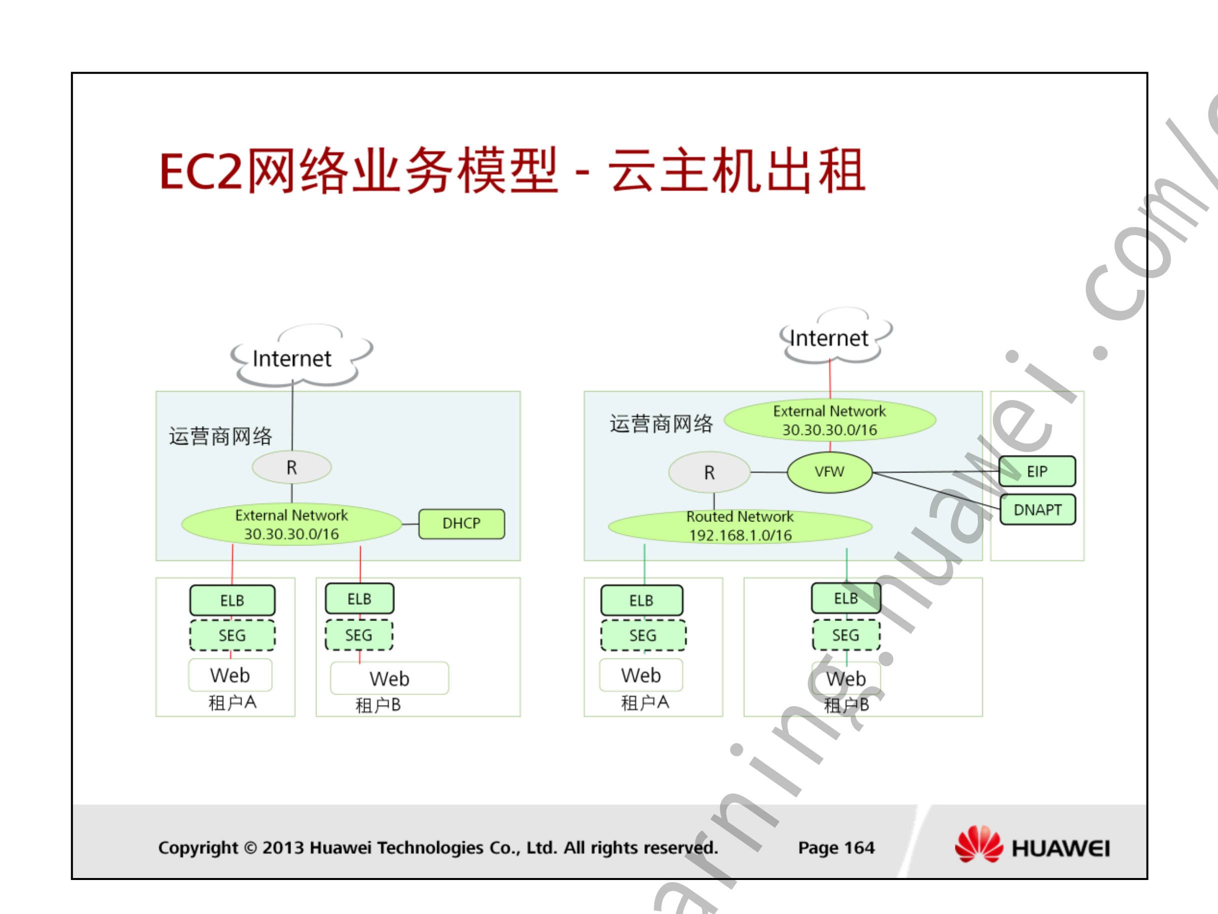
- 设计约束：

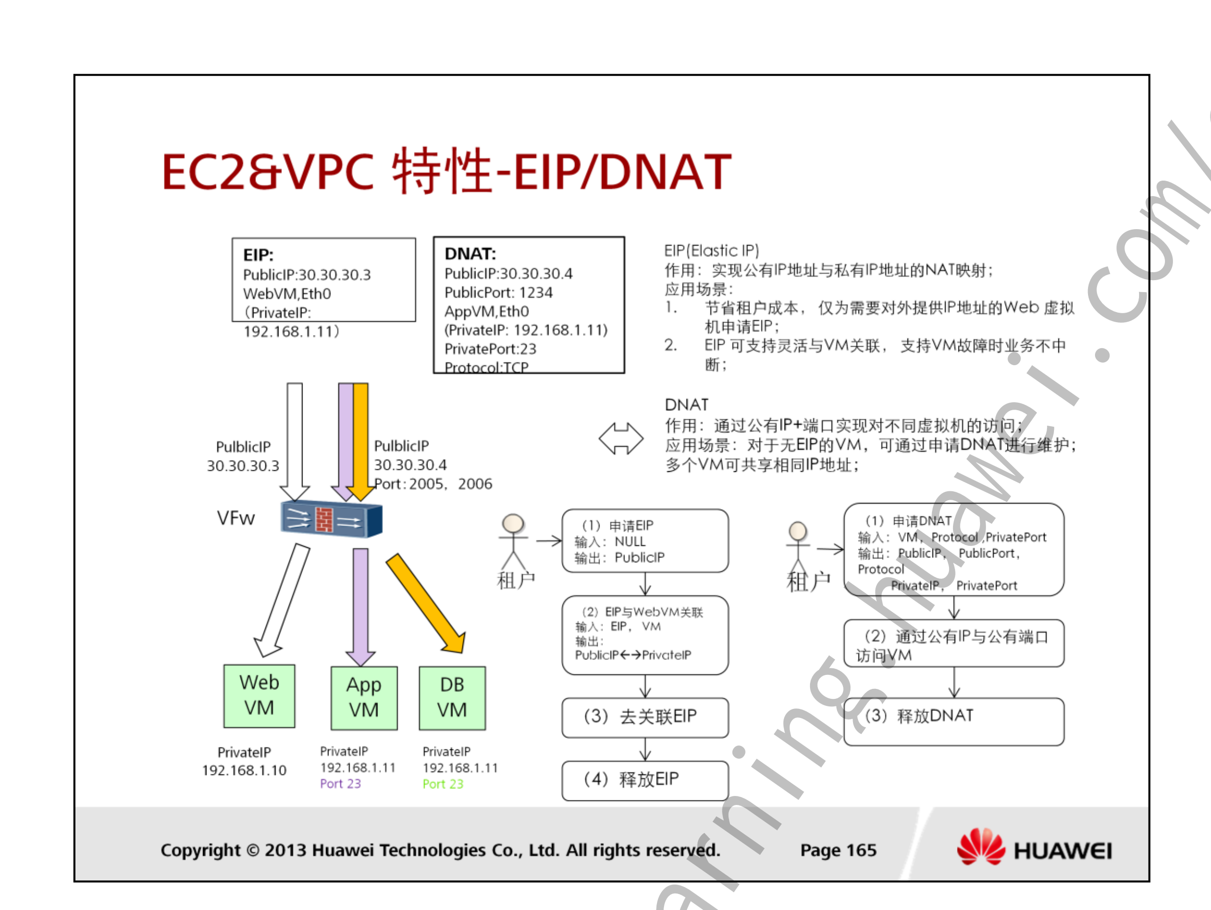
  1.VPC中没有Dhcp 不支持IP地址重叠子网， 子网是从系统定义的SubnetPool中自动分配；

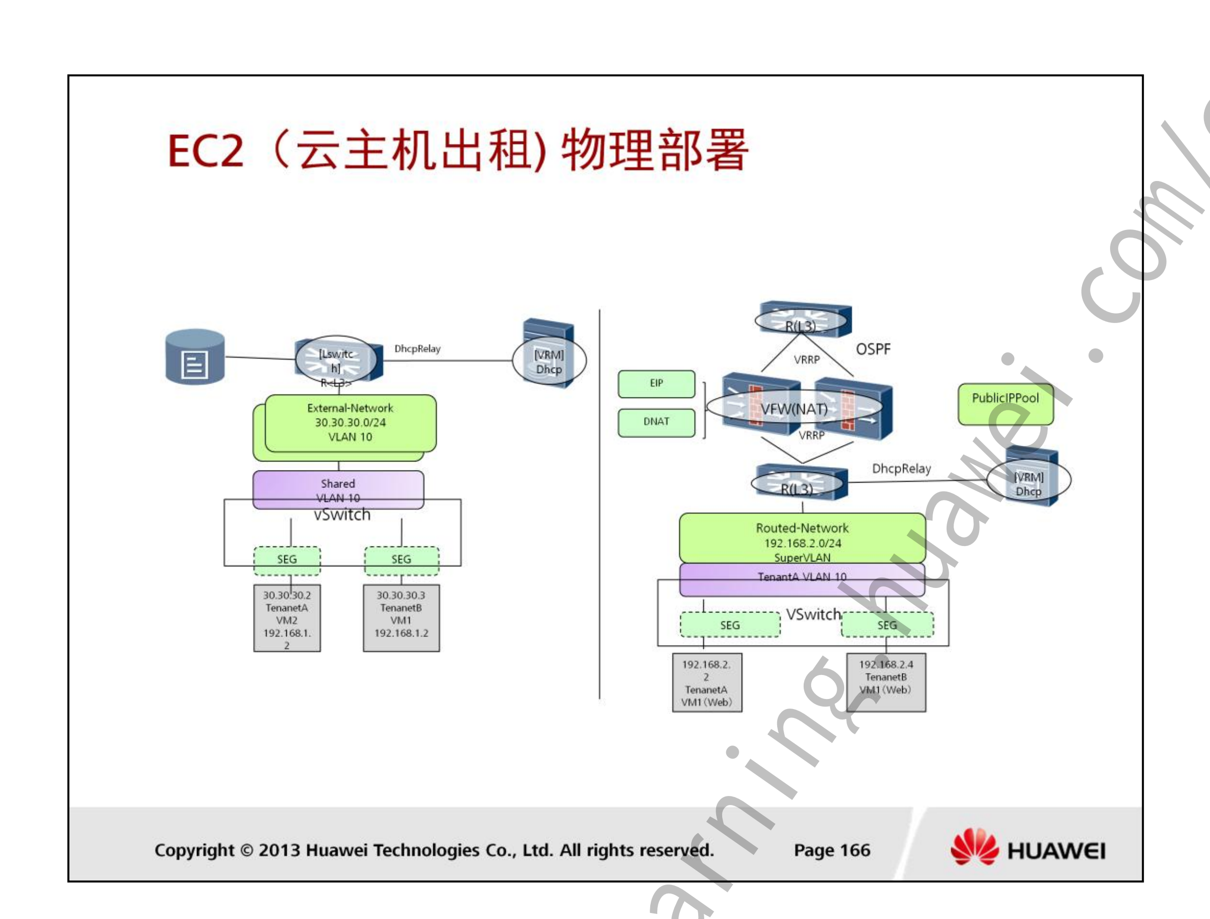
  2.EC2-Shared共享网络中定义的子网为安全组子网。安全组子网中定义了Segment。每个租户申请SEG时，系统会自动分配一个Segment。

  2.1 Routed Network：创建子网时，将子网与VFW关联，表示需要通过NAT才能访问公网

  2.2 Direct Network：创建子网时，子网不与VFW关联。


EC2网络业务模型 - 云主机出租
Internet
运营商网络
R
External Network
30.30.30.0/16
DHCP
ELB
SEG
Web
租户A
ELB
SEG
Web
租户B
Internet
运营商网络
External Network
30.30.30.0/16
R
VFW
EIP
DNAPT
Routed Network
192.168.1.0/16
ELB
SEG
Web
租户A
ELB
SEG
Web
租户B
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 164
HUAWEI


EC2&VPC 特性-EIP/DNAT
EIP:
PublicIP:30.30.30.3
WebVM,Eth0
（PrivateIP:
192.168.1.11）
DNAT:
PublicIP:30.30.30.4
PublicPort: 1234
AppVM,Eth0
(PrivateIP: 192.168.1.11)
PrivatePort:23
Protocol:TCP
EIP(Elastic IP)
作用：实现公有IP地址与私有IP地址的NAT映射；
应用场景：
1. 节省租户成本，仅为需要对外提供IP地址的Web 虚拟机申请EIP；
2. EIP 可支持灵活与VM关联，支持VM故障时业务不中断；
DNAT
作用：通过公有IP+端口实现对不同虚拟机的访问；
应用场景：对于无EIP的VM，可通过申请DNAT进行维护；多个VM可共享相同IP地址；
PulblicIP
30.30.30.3
PulblicIP
30.30.30.4
Port：2005，2006
VFw
Web VM
App VM
DB VM
PrivateIP
192.168.1.10
PrivateIP
192.168.1.11
Port 23
PrivateIP
192.168.1.11
Port 23
租户
（1）申请EIP
输入：NULL
输出：PublicIP
（2）EIP与WebVM关联
输入：EIP，VM
输出：
PublicIP←→PrivateIP
（3）去关联EIP
（4）释放EIP
租户
（1）申请DNAT
输入：VM，Protocol，PrivatePort
输出：PublicIP，PublicPort，Protocol
PrivateIP，PrivatePort
（2）通过公有IP与公有端口访问VM
（3）释放DNAT
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 165
HUAWEI


EC2（云主机出租）物理部署
DhcpRelay
[VRM] Dhcp
External-Network
30.30.30.0/24
VLAN 10
Shared
VLAN 10
vSwitch
SEG
SEG
30.30.30.2 TenanetA VM2 192.168.1.2
30.30.30.3 TenanetB VM1 192.168.1.2
R(L3)
OSPF
VRRP
EIP
DNAT
VFW(NAT)
PublicIPPool
DhcpRelay
[VRM] Dhcp
Routed-Network
192.168.2.0/24
SuperVLAN
TenantA VLAN 10
VSwitch
192.168.2.2 TenanetA VM1 (Web)
192.168.2.4 TenanetB VM1 (Web)
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 166
HUAWEI

EC2（云主机出租) 物理部署（续）

物理网络设备	直连外部网络	通过NAT连接外部网络
安全组子网网关	网关配置在汇聚交换机	网关配置在汇聚交换机
路由配置	默认路由为上行核心交换机	默认路由为防火墙下行接口IP地址；
VRF（NAT网关）	无	采用物理防火墙实现NAT。 支持旁挂与直挂模式 1）旁挂模式- 防火墙上行口与下行口连接到相同汇聚交换机； 2）直挂模式-防火墙上行口连接核心交换机， 下行口连接汇聚交换机；

1.虚拟防火墙采用手工配置；

1）虚拟防火墙采用手工创建；

2）虚拟防火墙上行接口、下行接口IP地址，VRRP手工配置

3）虚拟防火墙的OSPF手工配置



VPC物理部署硬件方案

LSW[L3]
OSPF
VRRP
[VRM]
Dhcp
DhcpRelay
R+IPGW
[VFW]
LSW[L2]
Routed Network
Routed Network
TenantA
VM
TenantA
VM
EIP
DNAT
FwAcl
ASPF

VPC特性

1.独占一个VFW，实现路由与外网互通

2.不同VPC的子网通过VFW进行隔离；

约束- R3C00 子网由系统分配；

物理网络设备	物理网络配置
汇聚交换机	1.连接物理防火墙下行接口配置2层VLAN； 2.连接物理防火墙的上行接口需要配置3层网关
防火墙	1.物理防火墙采用手工配置 1）VPN-Instance实现vFW，要求进行手工配置； 2）.VFW上行接口IP地址初始手工配置； - 主备VFW上行接口配置VRRP，实现路由备份； - VFW与交换机间采用OSPF动态发布公有IP地址主机路由； 2.VFW自动配置； 1）VPC 子网网关IP地址 2）EIP、SNAT、DNAT、ACL、ASPF

Page 168





目录

10. VPC



交换机防火墙配置

汇集交换机配置 → 防火墙基础配置 → 虚拟防火墙配置

汇集交换机配置：
- 交换机基础配置
- 交换机下行口trunk配置
- 防火墙安全域Trunk配置
- 和防火墙动态路由配置
- 安全组子网网关配置
- 安全组子网上行静态路由配置

防火墙基础配置：
- SSH用户信息
- SNMP配置
- 主备hrp配置
- 安全域配置
- trust、untrust域动态路由配置
- 开启限流策略

虚拟防火墙配置：
- 创建虚拟防火墙
- 默认转发策略
- untrust、管理域子接口配置
- trust子接口配置

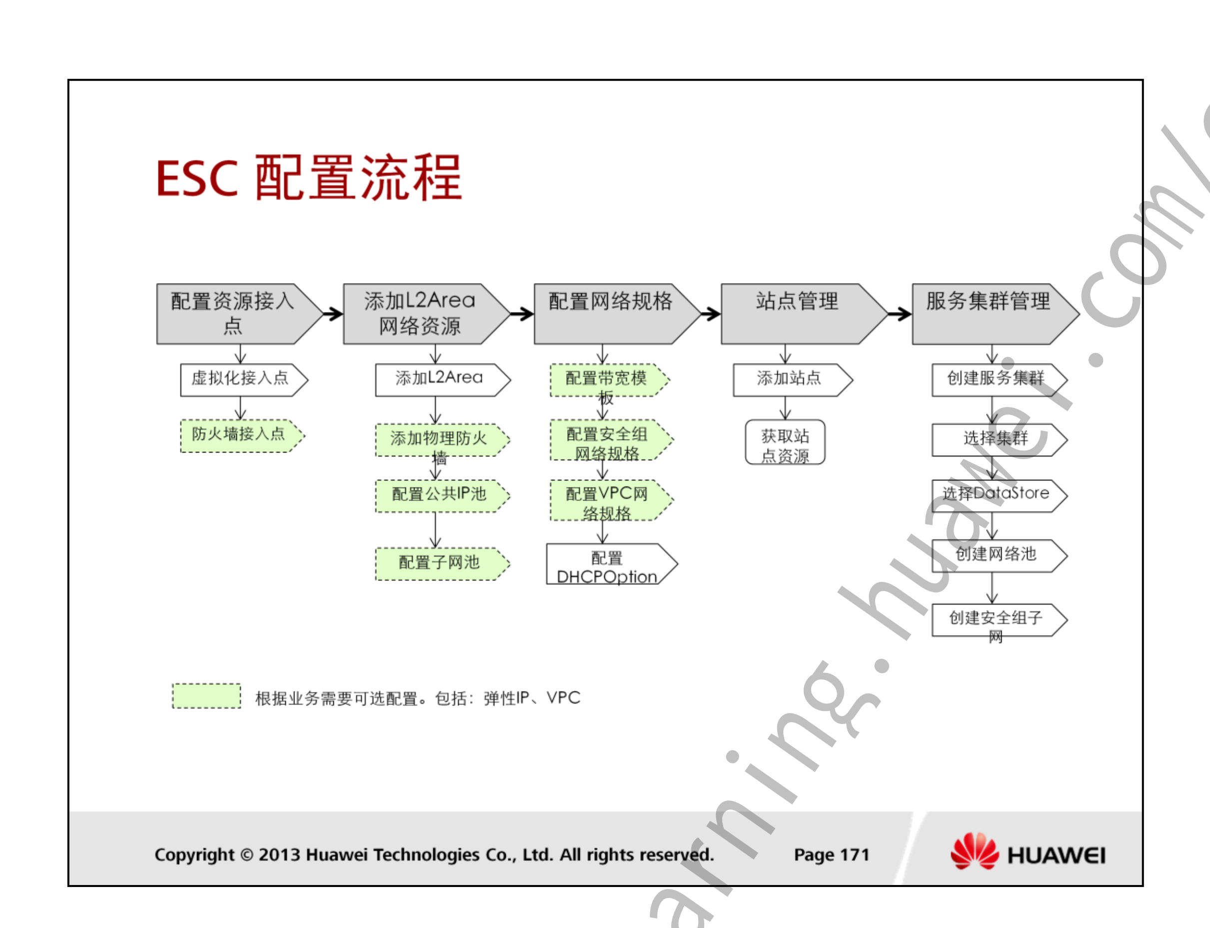
说明：

1、对于直连网络，不需要配置防火墙，以及交换机到防火墙的路由

2、交换机到防火墙OSPF动态路由，包括管理域以及防火墙untrust域

 安全组业务相关配置，没有安全组业务不需要配置

 Page 170 HUAWEI


ESC 配置流程
配置资源接入点
添加L2Area网络资源
配置网络规格
站点管理
服务集群管理
虚拟化接入点
防火墙接入点
添加L2Area
添加物理防火墙
配置公共IP池
配置子网池
配置带宽模板
配置安全组网络规格
配置VPC网络规格
配置DHCPOption
添加站点
获取站点资源
创建服务集群
选择集群
选择DataStore
创建网络池
创建安全组子网
根据业务需要可选配置。包括：弹性IP、VPC
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 171
HUAWEI

ESC 配置流程-资源接入点

目的：配置ESC链接VRM、UHM使用的链接参数，使ESC可以使用VRM、UHM提供的资源

虚拟化接入点：VRM级联后的链接信息。如果VRM没有级联，则为VRM本身的链接信息

防火墙接入点：防火墙管理节点的链接信息，目前为UHM的链接信息





HUAWEI

ESC 配置流程-L2Area管理

目的：网络资源和物理网络相关，配置每个物理二层网络相关的网络资源

L2Area：二层网络区域，以汇聚交换机区分，每对汇聚交换机为一个二层网络区域

物理防火墙、共有IP池、子网池为一个L2Area的资源

L2Area信息 > 配置物理防火墙 > 配置公有IP池 > 配置子网池 > 确认信息

请输入L2Area信息

* 名称: Mytest

描述: Mytest

下一步 取消

HUAWEI

ESC 配置流程-L2Area配置（1）

预置条件：完成物理防火墙的基础配置，包括虚拟防火墙配置

目的：添加物理防火墙连接信息，ESC通知FireMngr使用此信息连接防火墙并发现防火墙上的资源

说明：

1、没有配置防火墙接入点，不会显示物理防火墙配置

2、物理防火墙添加成功后，系统会自动发现虚拟防火墙资源

3、VPC业务、弹性IP业务需要用到物理防火墙

序号	管理IP	设备连接方式	用户名	SNMP版本	SNMP端口	SNMP超时时间(s)

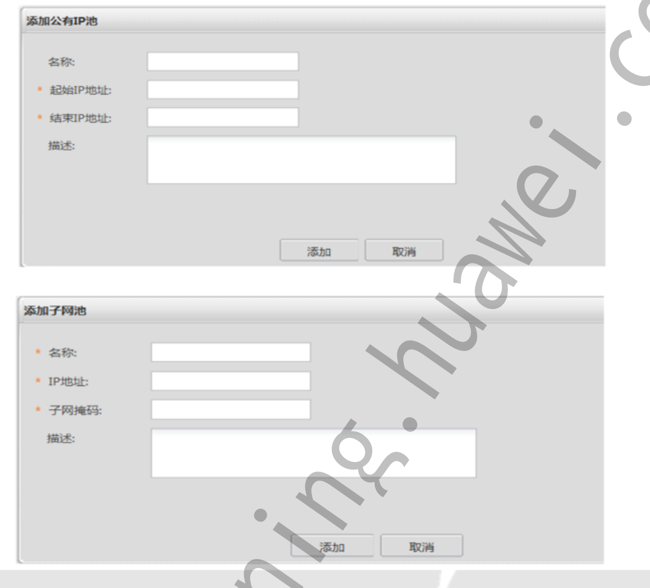
HUAWEI

ESC 配置流程- L2Area配置（2）

目的：配置L2Area可用的共有IP地址和子网池

公用IP池：弹性IP、公共IP、NAPT、VNC业务可使用的公共IP

子网池：VPC业务中，用户申请子网从子网池中分配。



说明：

1、没有配置防火墙接入点，不会显示共有IP池、子网池配置

2、公有IP池、子网池支持查询、修改和删除功能

ESC 配置流程-网络配置（1）

带宽模板配置：

1、管理员配置系统可用的带宽模板，供租户使用

2、弹性IP、VPC两种带宽模板类型，分别限制某一个弹性IP和整个VPC的出口带宽

3、需要首先配置物理防火墙

DHCP规格：

1、用于配置DHCPOption信息，在创建VM时，DHCPOption会初始化到VM中



HUAWEI

ESC 配置流程-网络配置（2）

安全组网络规格：配置安全组业务使用的虚拟防火墙、弹性IP默认带宽模板、DNAT端口范围

VPC网络规格：配置VPC业务的弹性IP默认带宽模板、DNAT端口范围

说明：只有配置防火墙接入点后，才能启用安全组的弹性IP业务、配置VPC网络规格

提示：配置VPC-Network网络规格。

网关策略： 防火墙作3层网关

启用弹性IP业务： 已启用

弹性IP配置

默认弹性IP最大接收带宽模板：

默认弹性IP最大发送带宽模板：

DNAT配置

* DNAT的起始端口： 1

* DNAT的结束端口： 65535

提示：配置安全组网络规格。

网关策略： 交换机作3层网关

启用弹性IP业务： 启用

* L2Area: l2-base

* 虚拟防火墙：

	名称	使用状态	物理防火墙	最大接收带宽(Mbit/s)	最大发送带宽(Mbit/s)	ACL个数	L2Area
◉	vpn96	空闲	Fw_A	-1	-1	0	l2-base

弹性IP配置：

默认弹性IP最大接收带宽模板：

默认弹性IP最大发送带宽模板：

DNAT配置：

* DNAT的起始端口： 1

* DNAT的结束端口： 10

HUAWEI

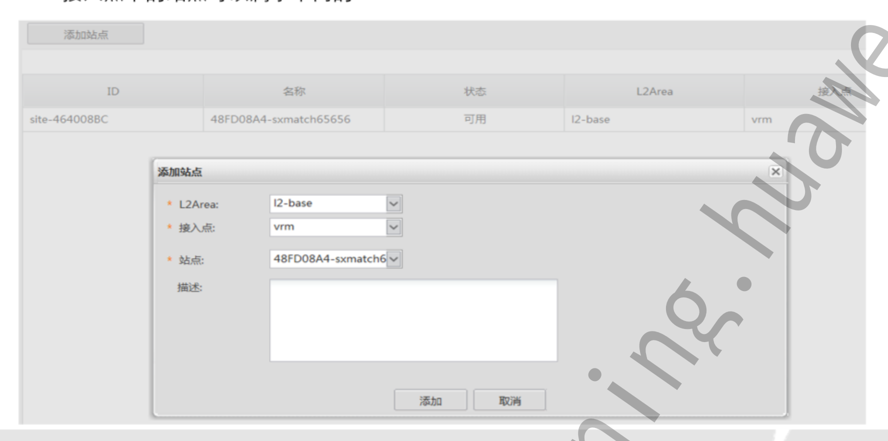
ESC 配置流程-添加站点

站点：VRM级联后，级联节点管理的其他VRM

说明：

1、一个站点只能在一个L2Area

2、接入点下的站点可以属于不同的L2Area



HUAWEI


ESC配置流程-添加服务集群
1、ESC的一个服务集群，对应一个AvailableZone
2、服务集群和VRM的集群一一对应
3、创建服务集群选择的数据存储，为VRM上集群可用的存储
基本信息
选择集群
选择数据存储
输入服务集群的基本信息。
名称:
test
描述:
下一步
取消
配置网络池
选择当前可用集群资源。
选择站点
site-464008BC
选择集群
名称
内存总大小(MB)
cluster1
45223
选择可用数据存储。
状态
正常
914
22
892
否
本地存储
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 179
HUAWEI

ESC 配置流程-添加服务集群

目的：配置一个服务集群可以使用的VRM上的VLAN资源

说明：

1、对于一个集群，ESC只能使用和其关联的一个DVS上的VLAN

2、网络池为DVS关联的VLAN池的子集

3、在服务集群的属性页，可以删除、添加网络池中的VLAN段



HUAWEI

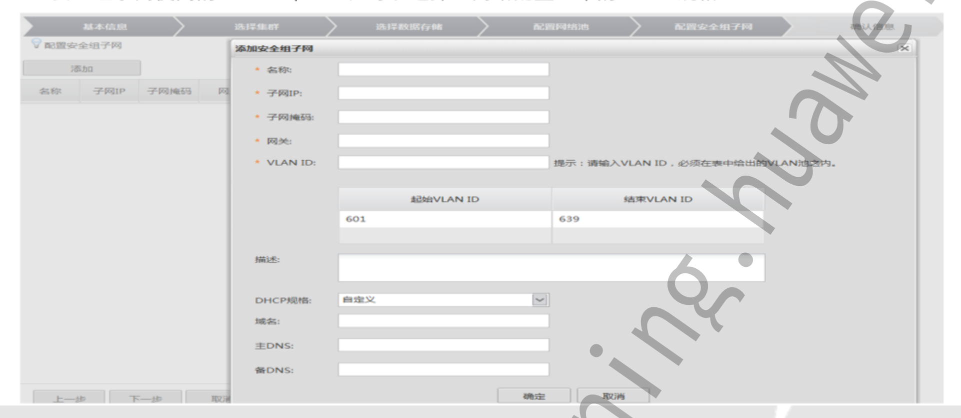
ESC 配置流程-安全组子网

目的：配置一个服务集群中，安全业务使用的子网，以及子网对应的VLAN、DHCPOption信息

说明：

1、安全组子网使用的VLAN在服务集群的网络池内

2、安全组子网使用的DHCPOption，可以选择“网络配置”中的DHCP规格

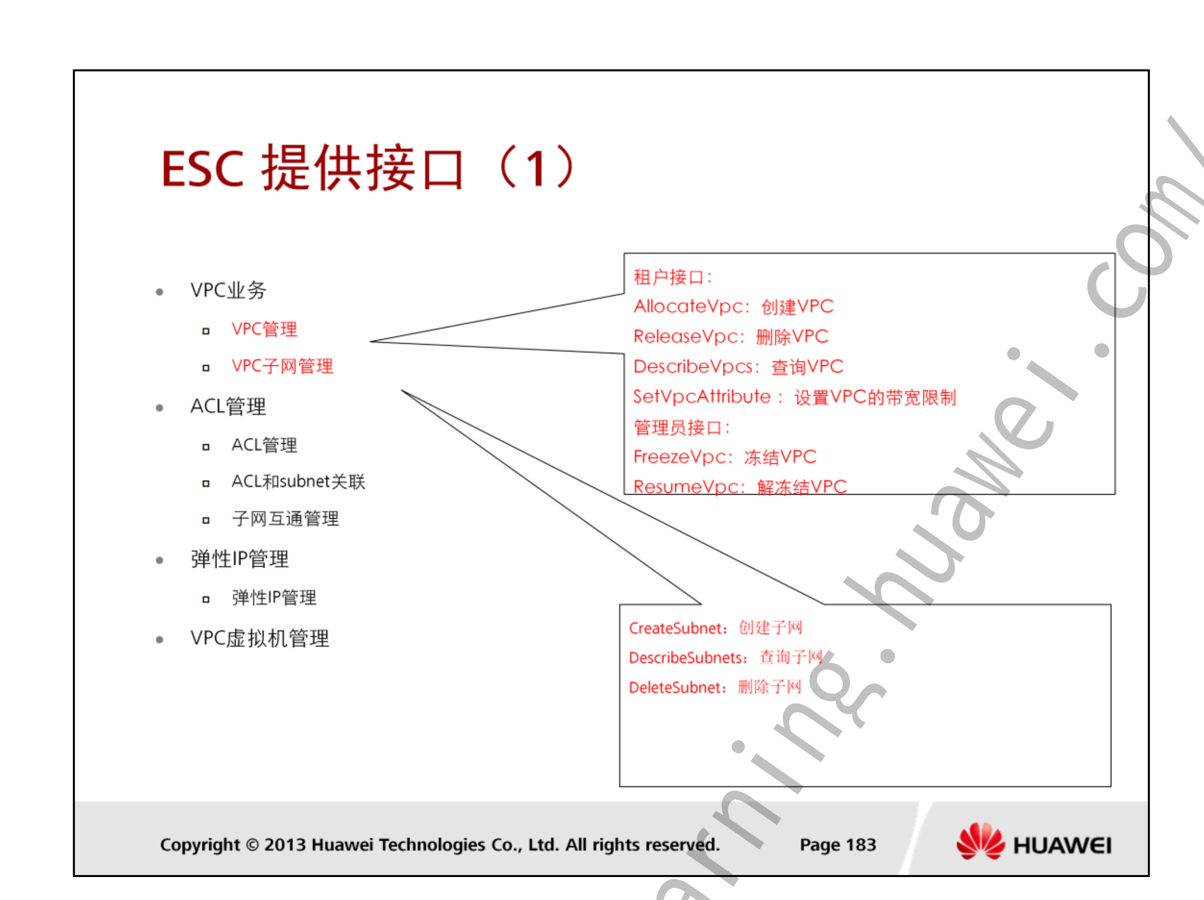


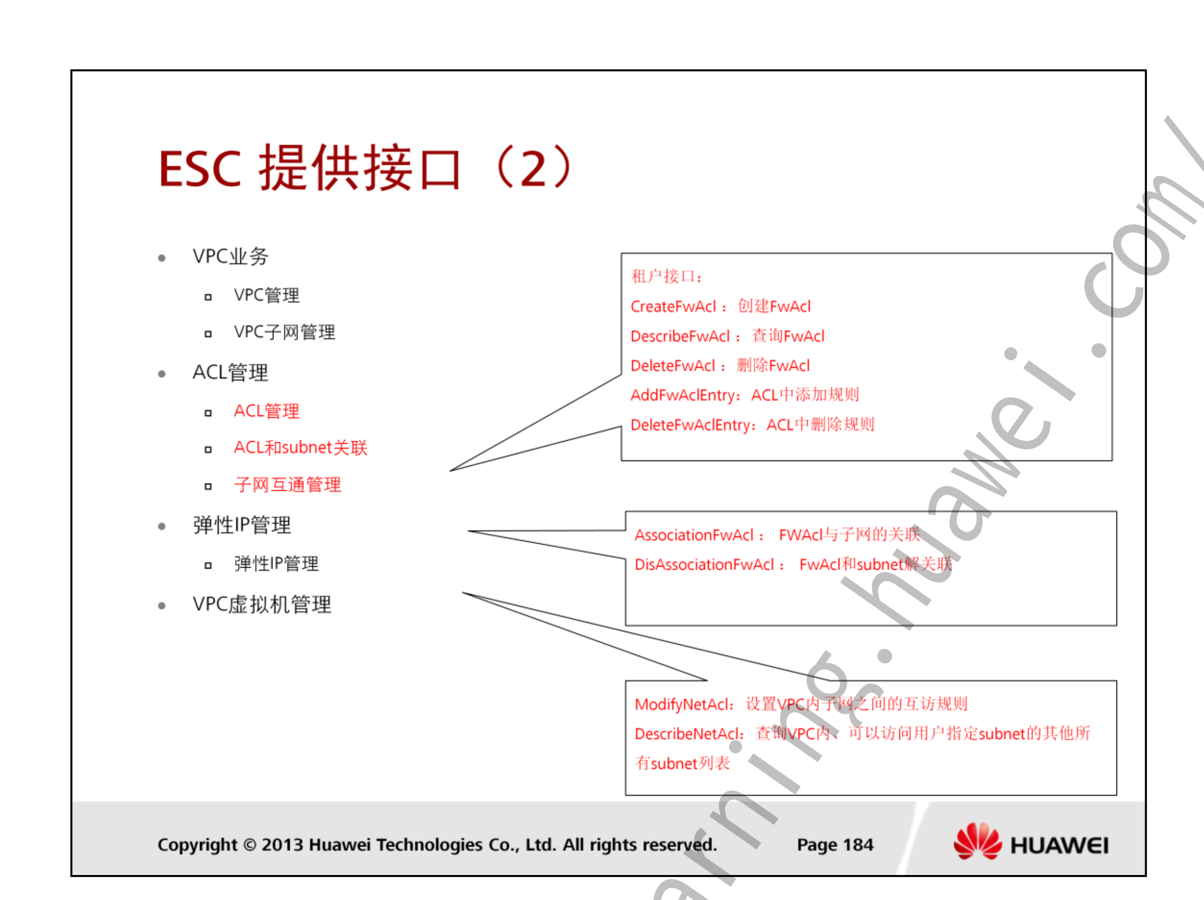


ESC 提供接口

- VPC业务
  - VPC管理
  - VPC子网管理
- ACL管理
  - ACL管理
  - ACL和subnet关联
  - 子网互通管理
- 弹性IP管理
  - 弹性IP管理
- VPC虚拟机管理




ESC 提供接口（1）
VPC业务
VPC管理
VPC子网管理
ACL管理
ACL管理
ACL和subnet关联
子网互通管理
弹性IP管理
弹性IP管理
VPC虚拟机管理
租户接口：
AllocateVpc：创建VPC
ReleaseVpc：删除VPC
DescribeVpcs：查询VPC
SetVpcAttribute：设置VPC的带宽限制
管理员接口：
FreezeVpc：冻结VPC
ResumeVpc：解冻结VPC
CreateSubnet：创建子网
DescribeSubnets：查询子网
DeleteSubnet：删除子网
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 183
HUAWEI


ESC 提供接口（2）
VPC业务
VPC管理
VPC子网管理
ACL管理
ACL管理
ACL和subnet关联
子网互通管理
弹性IP管理
弹性IP管理
VPC虚拟机管理
租户接口：
CreateFwAcl： 创建FwAcl
DescribeFwAcl： 查询FwAcl
DeleteFwAcl： 删除FwAcl
AddFwAclEntry：ACL中添加规则
DeleteFwAclEntry：ACL中删除规则
AssociationFwAcl： FWAcl与子网的关联
DisAssociationFwAcl： FwAcl和subnet解关联
ModifyNetAcl：设置VPC内子网之间的互访规则
DescribeNetAcl：查询VPC内、可以访问用户指定subnet的其他所有subnet列表
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 184
HUAWEI

ESC 提供接口（3）

- VPC业务
  - VPC管理
  - VPC子网管理
- ACL管理
  - ACL管理
  - ACL和subnet关联
  - 子网互通管理
- 弹性IP管理
  - 弹性IP管理
- VPC虚拟机管理
  - 管理虚拟机

租户接口：
AllocateAddress：申请弹性IP
ReleaseAddress：释放弹性IP
AssociateAddress：绑定弹性IP
DisassociateAddress：解绑定弹性IP
DescribeAddresses：查询弹性IP
SetIPBandWidth：设置弹性IP带宽
DescribeIPBandWidth：查询弹性IP带宽
管理员接口：
FreezeEip：冻结弹性IP
ResumeEip：解冻结弹性IP

创建VPC虚拟机：
指定虚拟机所在的VPC，虚拟网卡所在的subnet
查询虚拟机：
返回虚拟机所在的subnet，虚拟网卡分配到的IP



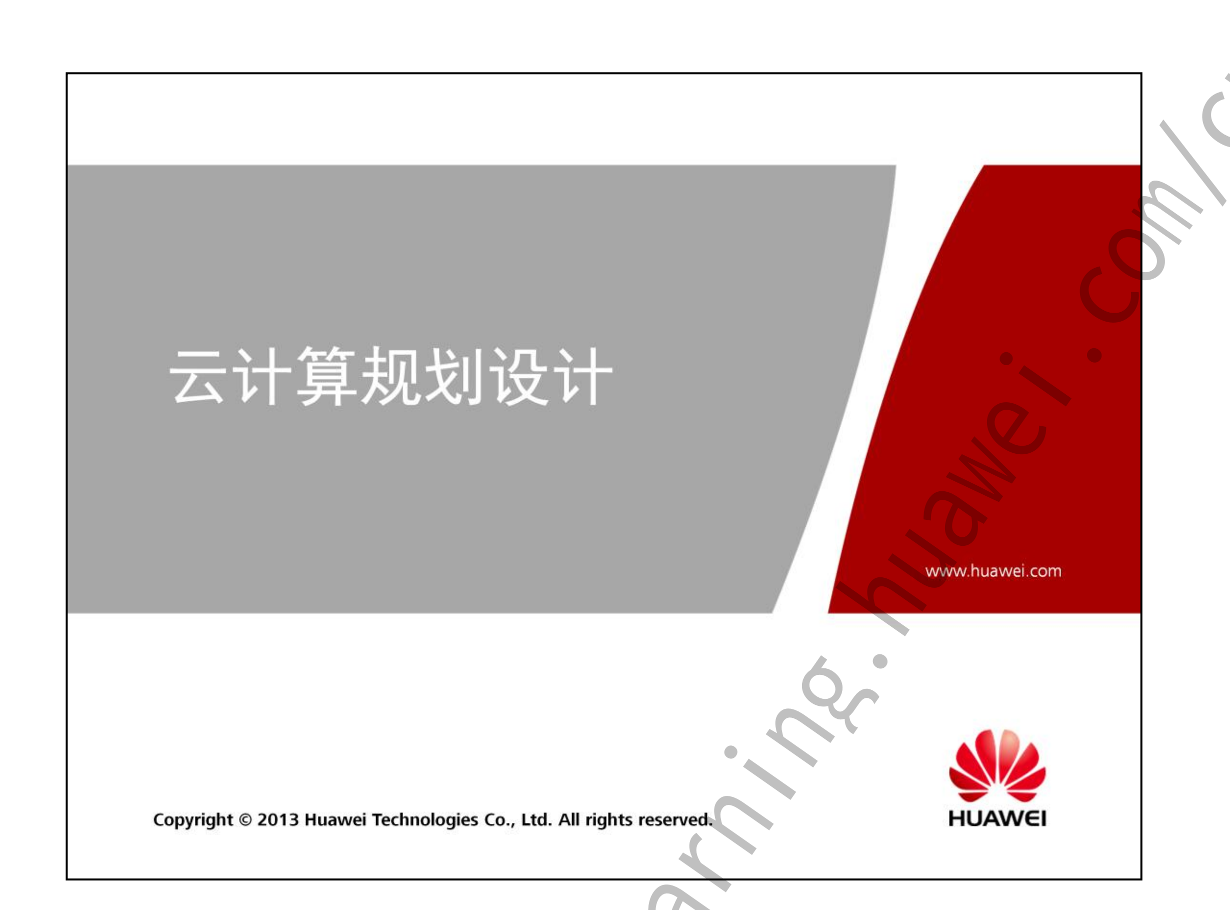
总结

- FusionStorage的原理和应用
- GPU直通方案的原理和应用
- 应用虚拟化的原理和应用
- 应用自动部署/应用弹性伸缩的原理和应用
- 自动精简配置的应用
- ELB原理和应用
- VPC原理和应用



Thank you

www.huawei.com


云计算规划设计
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

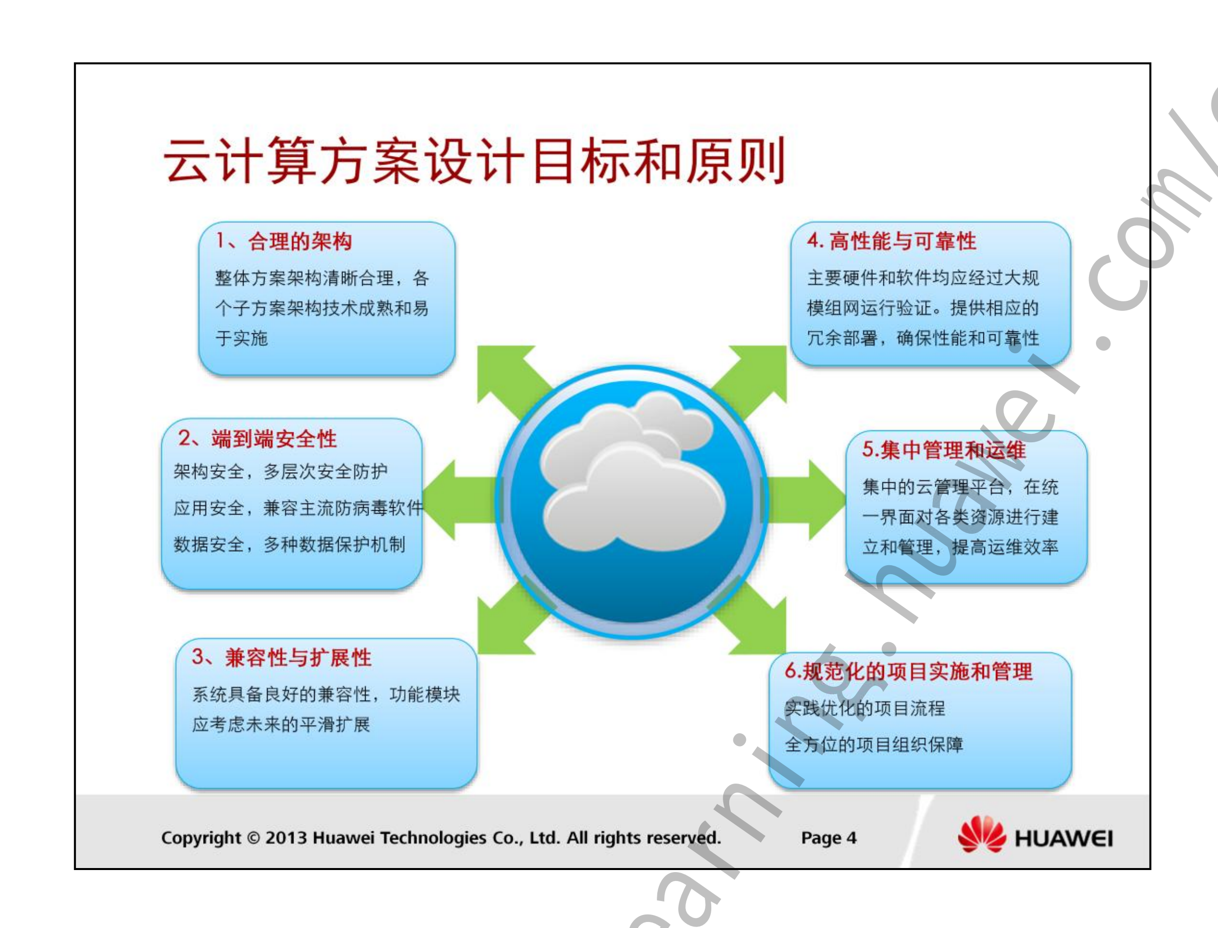
- 学完本课程后，您将能够:
  - 熟悉桌面云的场景与需求分析；
  - 熟悉数据中心虚拟化的场景与需求分析；
  - 按项目需求分析写出对应的技术建议书；
  - 熟悉技术建议书各个章节、并能独立写作；
  - 精通桌面云的容量规划与配置；
  - 精通服务器虚拟化的容量规划与配置；





目录

1. **设计目标和原则**
2. 需求分析
3. 容量规划
4. 系统方案设计
5. 网络方案设计
6. 安全方案设计
7. 灾备方案设计
8. 运维方案设计
9. 案例学习



信息化为什么要上云计算、桌面云，可以从以下面几方面讲述云计算的优势：

- 高安全性

  安全接入，分权分域，集中管控：桌面云提供一体化的安全准入控制，集成现有的安全规程，依据相应的权限策略实现对不同安全域，不同接入类型用户的集中管控，保障核心数据，以及对不同业务资源的灵活分配、分权管理与审计。

- 高效体验

  桌面云系统提供最佳的访问体验，用户不再受PC、Windows系统的频繁故障的影响。实现不同网络环境的一致访问体验，提升桌面的可用性与连续性。桌面云系统简单，易用，并提供友好用户界面与自助维护界面。

- 高可靠性

  采用先进虚拟化技术，资源池化，所有设备均应经过大规模组网运行验证。系统的业务、管理、存储功能应该由独立的平面承载，所有设备、模块节点具备冗余部署能力，确保系统及业务的可靠运行，并且系统应具有平滑扩容的能力。

- 高可服务性

  降低运维成本，提高工作效率，减轻管理维护人员的工作强度与不必要的的重复劳动。桌面云系统将应用、桌面的升级、变更、维护等工作交由后台统一管理与运行；具备良好的综合定位分析及故障恢复能力，从而降低对业务的影响。供应商具备为项目长期服务和保障的能力。

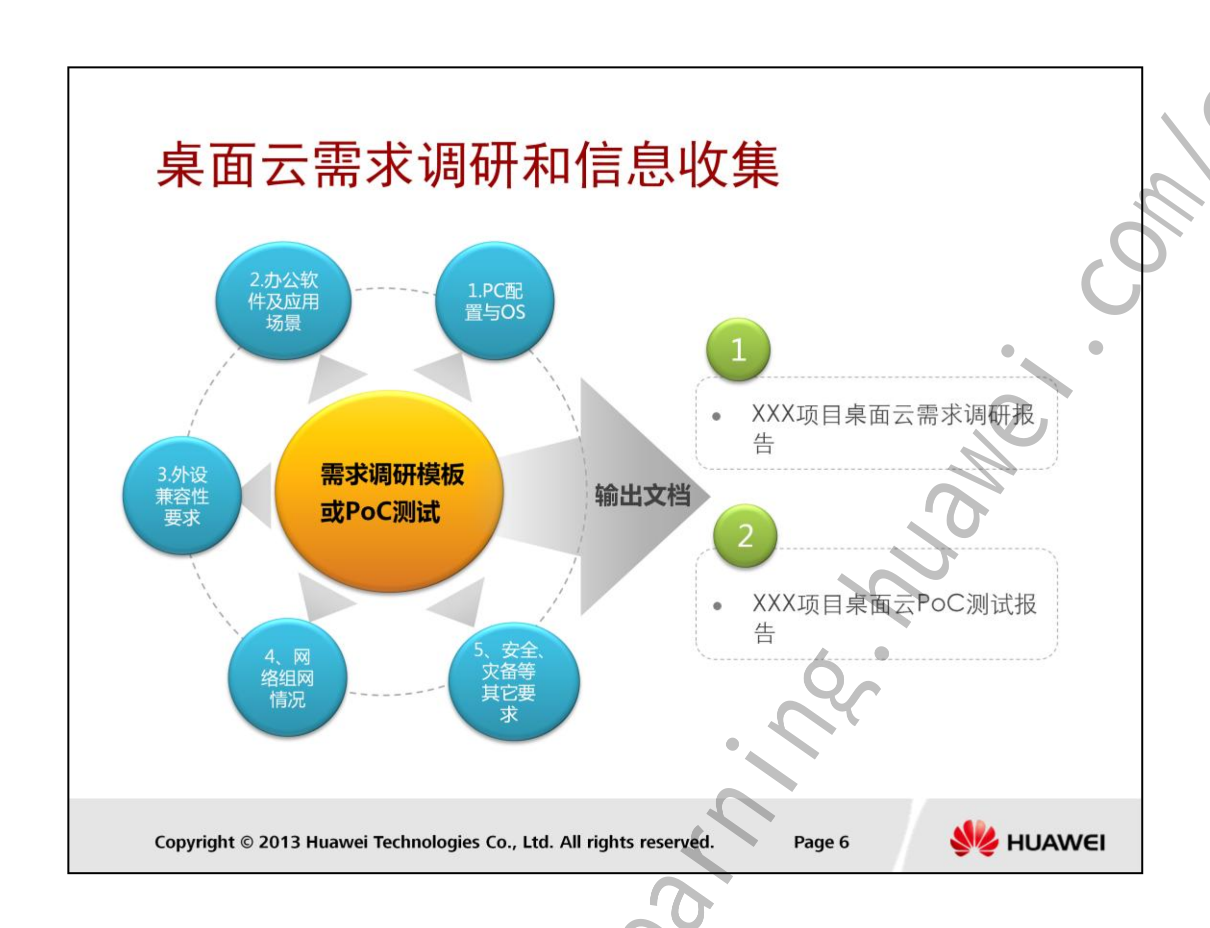


目录

 Page 5







云计算项目主要有两块市场：

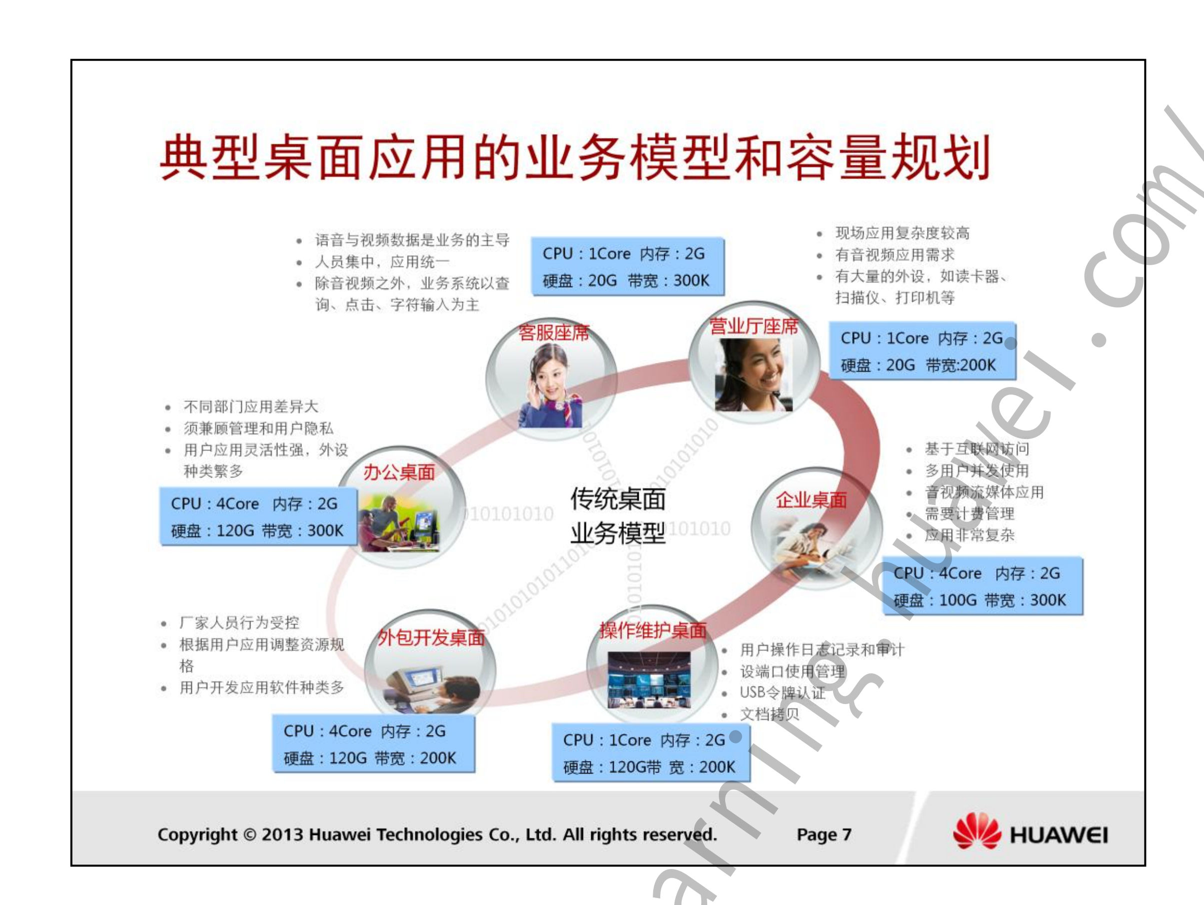
一是数据中心虚拟化， 二是桌面云。

对于桌面云市场项目，先从需求调研开始，

1.桌面云调研模板：《华为桌面云解决方案项目需求调研模板 v1.0.xlsx 》参见：http://3ms.huawei.com/mm/docMaintain/mmMaintain.do?method=showMMDetail&f_id=DC13020612420013

2.对于一些客户，没有接触过桌面云，或者验证是否适用于客户的办公场景，需要PoC测试。

POC测试：即Proof of Concept，是业界流行的针对客户具体方案和应用的验证性测试。



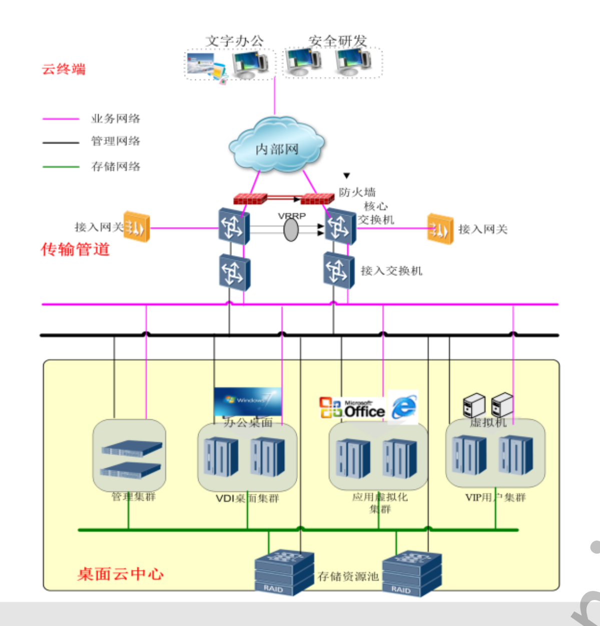
- 适用场景：PC办公场景， 除了以下场景。
- 图形桌面、视频播放支持程度不是很好。



目录



桌面云总体方案



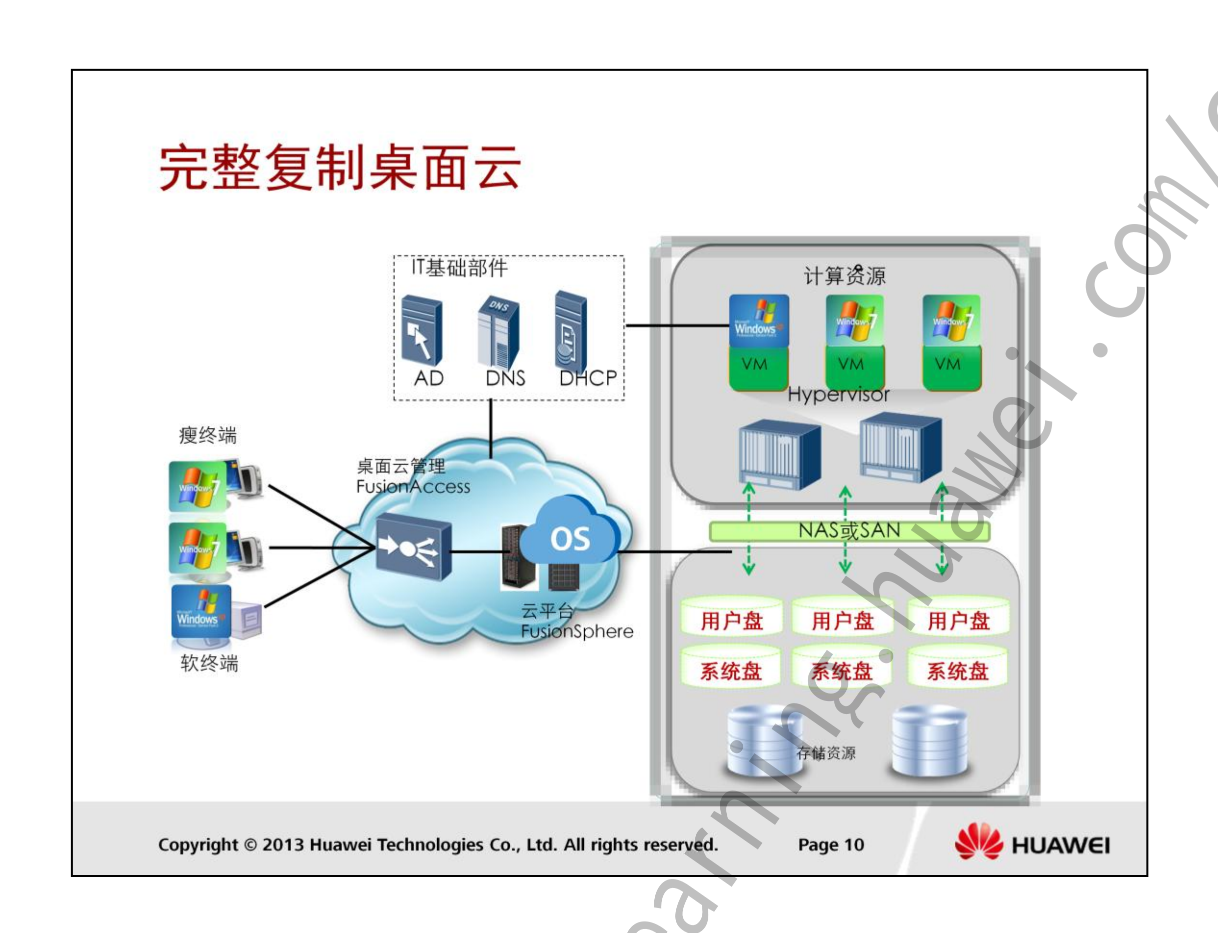
方案要点

- 明确桌面云的应用场景。
- 按照应用场景需求选择完整复制、链接克隆、PvD、应用虚拟化方案。
- 按照迁移策略、应用场景来划分集群。
- 体现桌面云的高安全，高可靠，方便运维。
- 其它如备份，移动办公，分支机构要求也在总体方案中简要描述方案。

 Page 9



- **设计思路：**
  - 资源池化，统一运维
  - 普通用户、VIP用户、应用虚拟化三个独立集群。
  - 业务、存储、管理三网隔离，保证安全
- **设计目标：**
  - 高效体验，兼容PC。
  - 高安全、高可靠
  - 高性能、平滑扩容
  - 集中自动化运维



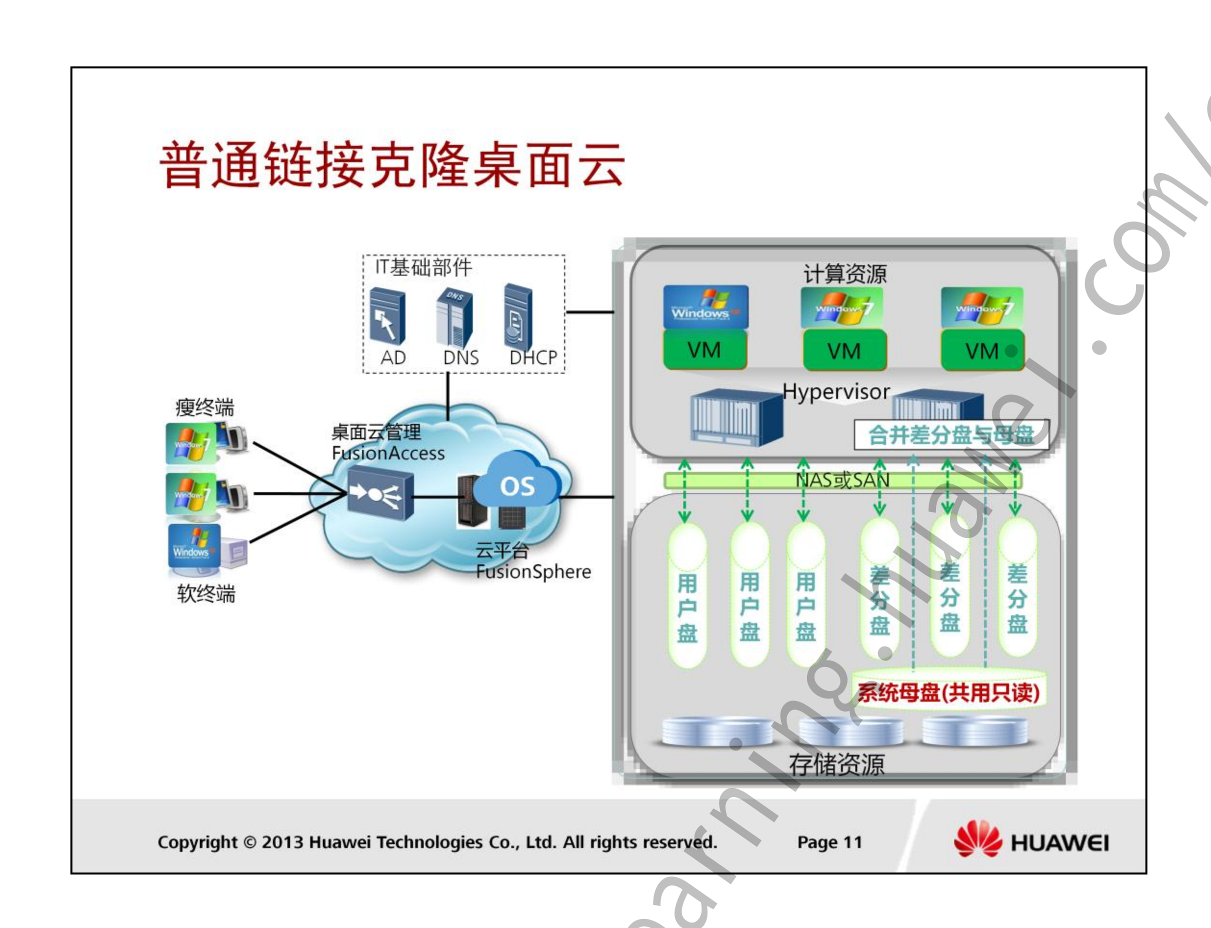
- 完全克隆虚拟桌面在创建时，系统会给这个虚拟桌面分配一份独立系统盘空间，并将虚拟机模板完整复制到系统盘上。这样每个完整复制虚拟桌面都有单独的系统盘与用户数据盘。

方案要点

- 每个用户的系统盘、数据盘都独立，安全性高，个性化强。外设兼容丰富。

适用场景

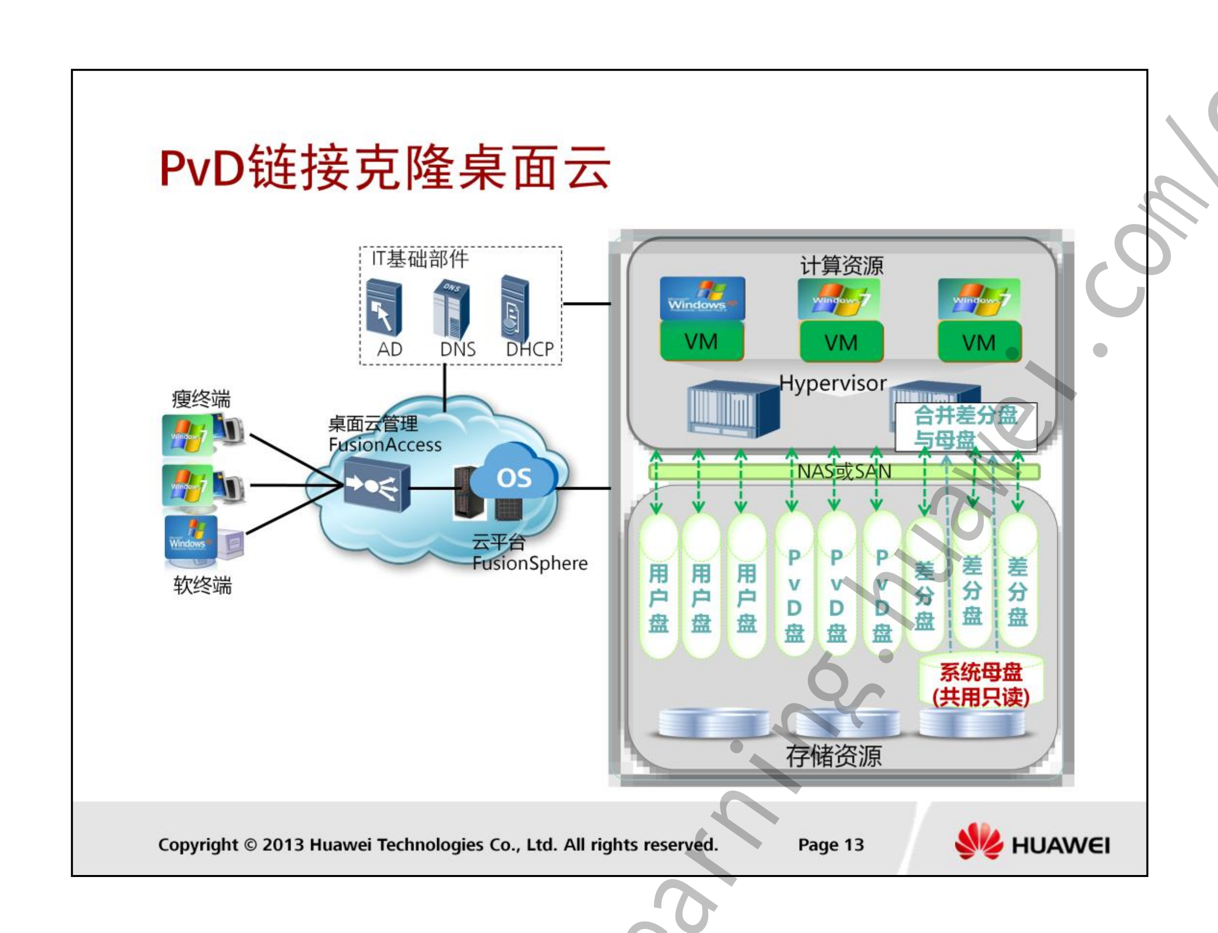
- 行政办公、研发办公、营业厅、呼叫中心、轮班值办公



方案要点：系统盘共用，差分盘保存差异数据。重启可配置是否清除差分盘，还原系统。

适用场景：电教室、公共上网区、阅览室。

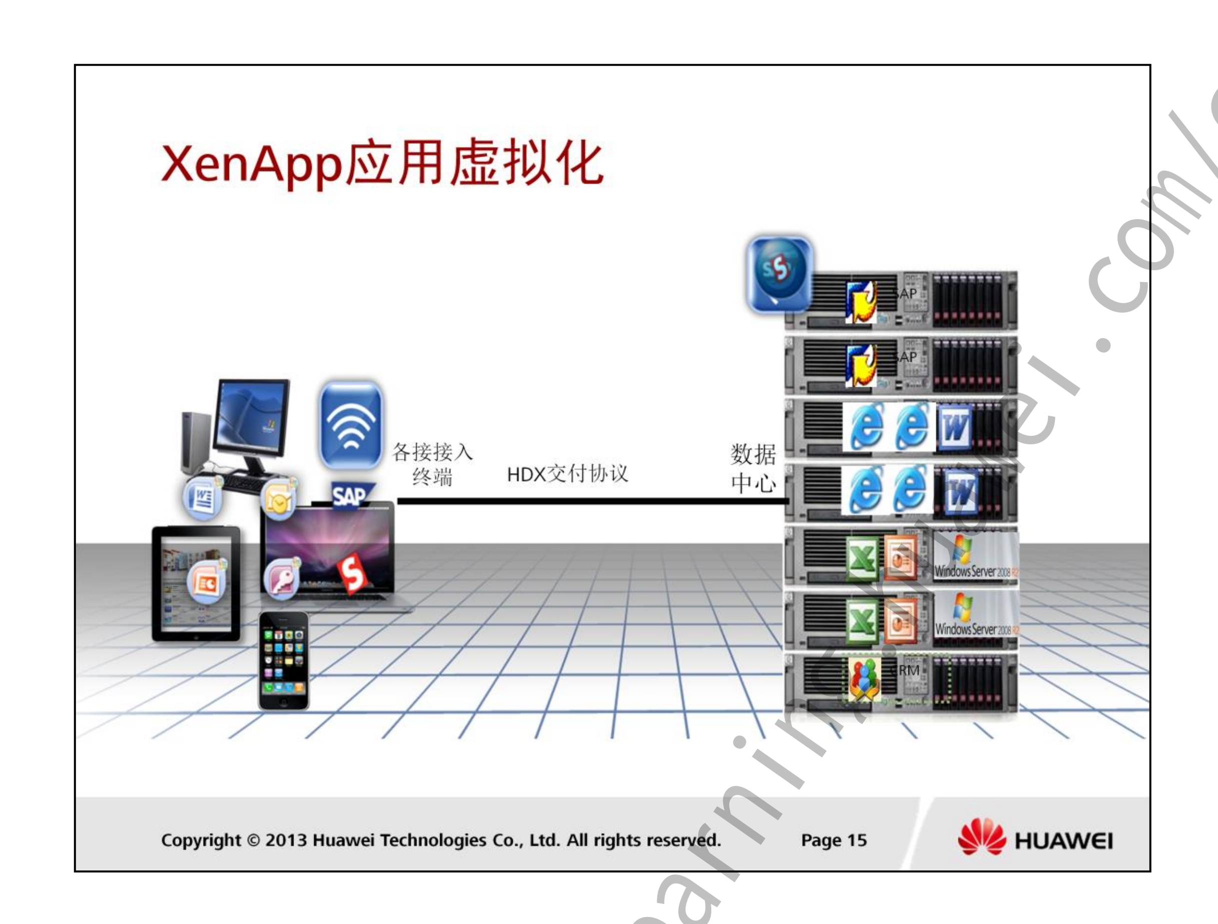
- 普通链接克隆桌面与全克隆桌面的区别主要在于系统盘的存储上。链接克隆桌面的虚机共享一个相同的系统母盘，每台虚拟机系统盘的不同部分（如工作临时缓存数据、个性化配置（C:\User(在Windows 7中)或C:\Documents and Settings(在Windows XP中)）、临时安装的个性化应用程序（C:\Program Files）等）都保存在差分盘中。并且通过将母盘和差分盘组合映射为一个链接克隆盘作为虚拟机的整个系统盘（即C盘），提供给虚拟机使用。对于虚拟机的差分盘，可以配置更新还原策略，还原策略可配置为手动还原与重启还原。
- 由于系统母盘是很多桌面共用，所以对于系统母盘需要很高的读性能。华为虚拟化平台对于链接克隆母盘提供iCache加速功能。可以将系统母盘的热点数据缓存到服务器本地磁盘、或本地内存中。 这样就减小了对共享存储的性能冲击。
- 使用普通链接克隆桌面的每个用户仍可以挂载不同的用户数据盘，用来保存数据。普通链接克隆桌面除拥有传统VDI的安全隔离、外设兼容性、工作体验外，还有以下优势。



方案要点：系统盘共用，PvD盘保持个性化配置文件，程序安装。重启可配置是否清除差分盘，还原系统。PvD盘仍保留。

适用场景：个性化办公、营业厅、呼叫中心。

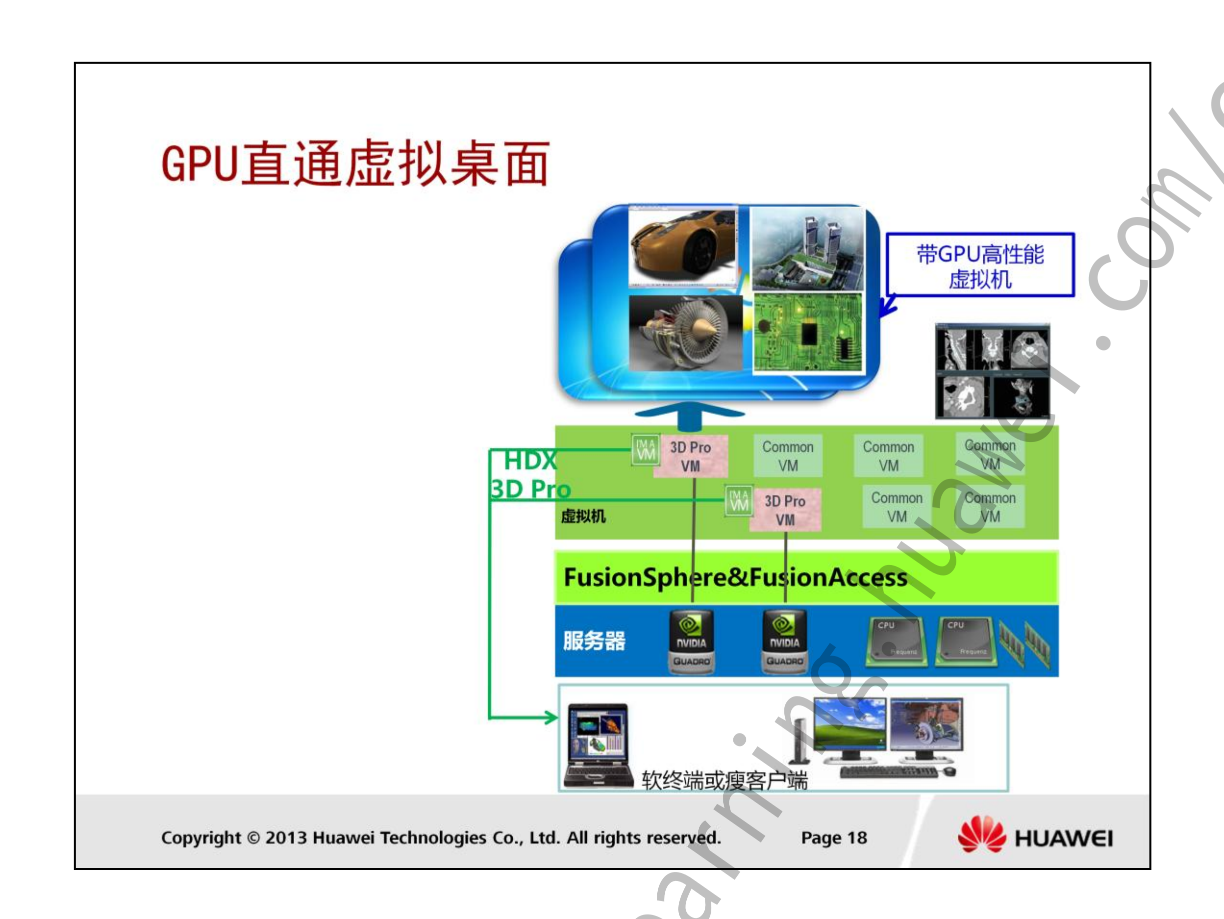
- 普通链接克隆桌面在操作系统与应用软件更新、升级上有很大优势，非常适用于无状态桌面应用场景，如会议室桌面、网吧等；但对链接克隆虚拟机进行系统更新时，保存在差分盘中的个性化数据会清除，不适合个性化桌面场景。
- Personal vDisk是面向虚拟桌面的一种个性化解决方案，它保留了池桌面单映像管理功能，同时允许用户安装应用程序和更改自己的桌面设置；它将对用户的VM所做的所有更改重定向到连接至用户的VM的独立磁盘（即个人虚拟磁盘），从而将每位用户的个性化设置分隔开来。个人虚拟磁盘中存储的内容在运行时与基础VM（母卷及差分卷所呈现的系统盘）中的内容混合在一起，以提供一致的体验,非常适合于个性化桌面场景。
- 对于PvD链接克隆虚拟机，提供了系统更新操作，管理员可以统一对链接克隆虚拟机组中的虚拟机进行软件更新操作，完成链接克隆虚拟机的系统母卷更新。
- PvD链接克隆池化桌面支持静态池。



方案要点：Windows 2008系统上应用发布，桌面发布。

适用场景：移动办公，应用发布，Windows 2008桌面。

- **XenApp应用虚拟化的特点：**
- 华为XenApp应用程序虚拟化，可以使Windows各种应用在服务器侧集中管理和发布，用户不需要在本地安装，就可以使用这些应用程序。应用程序安装在XenApp服务器上，并发布给用户或群组，给用户提供虚拟应用服务。所有XenApp服务器及其他配套组件服务器均部署在FusionSphere云平台上。
- **XenApp应用虚拟化的优势：**
- 简化IT管理：将应用和数据从个人设备转移到数据中心，XenApp将应用程序集中在数据中心，可以降低管理成本，提高IT向分散用户交付应用的响应速度，加强应用和数据的安全性。
- 简化用户使用：将应用和数据从个人设备转移到数据中心后，所有应用和数据都在一个安全的位置进行维护、备份和管理。分散用户不再需要投入应用维护、数据备份、应用和数据的管理。
- 按需访问：用户可以通过TC、PAD、智能终端等多种设备即时、按需地使用应用。
- 应用虚拟化特点：
- 对应用程序要求支持在Windows 2008 R2上运行，并且支持多实例；



方案要点：

1、每个图形加速虚拟机绑定一个GPU满足3D应用的图形渲染，服务器的剩余CPU资源可以创建不带GPU的普通虚拟机。

2、服务器采用 4*Q2000或2*Q4000每块E9000刀片。2*Q2000每RH2288机架服务器。

3、客户端采用高性能TC或PC

适合场景：3D图形处理，图形处理的桌面比例相对较低（10%以下）

- **服务器端：**
  - 通过华为FusionSphere虚拟化技术，使得单一物理机上可以运行多个虚拟机，最大化利用服务器资源
  - GPU Passthrough 技术可以物理服务器的GPU卡直接映射至虚拟机
  - 虚拟机可以独占GPU的资源，最大化满足3D应用的图形渲染和计算需求
  - 服务器的其他资源仍然可以创建普通虚拟机，这些普通虚拟机同高性能图形一期被华为Vdesktop 统一管理 。
  - 用户可以根据实际需求为所创虚机绑定或解除绑定GPU资源



1. 设计目标和原则
2. 需求分析
3. 系统方案设计
4. **容量规划**
5. 网络方案设计
6. 安全方案设计
7. 灾备方案设计
8. 运维方案设计
9. 案例学习

Page 19



- 容量规划的三个方面：服务器的容量、存储的容量、网络带宽的容量

桌面云容量规划的步骤

第一步：确认虚拟机规格

参数	vCPU	内存(GB)	IOPS	磁盘	网卡个数	并发率	用户总数
数值	2	4	7	系统盘=40G 数据盘=80G	1*1Gbps	75%	500



第二步：根据虚拟机密度基线计算服务器数量

第三步：根据虚拟机规格计算存储容量

虚拟桌面密度测试方法一：LoginVSI

负载类型	VSI业务负载详细定义
轻载	运行比较少的应用，在使用完之后立即关闭，需要更低CPU和内存消耗；轻载模拟同时只打开2个应用；仅使用IE，Word和Outlook三种应用；空闲时间大概是1:45分钟；
中载	是VSI默认负载；该负载模拟一个使用Office、IE和PDF的中等程度；会话启动，每隔12分钟重复一次；每次循环过程中每隔2分钟计算一次响应时间；中载同时打开5个应用软件；中载的打字速度是每个字符160毫秒；有2分钟的空闲时间。
重载	重载需要更多的CPU和内存消耗，因为更多的应用程序会在后台运行；重载的压力是基于中载之上；与中载的不同点在于：打字速度是130ms一个字符；空闲时间仅仅只有40秒；重载同时打开8个应用程序；
其他负载	多媒体负载：模拟一个多媒体用户； 组合负载：在一个用户会话中将不同负载组合在一起； 内核负载：是一个完全空的负载。该负载会执行登录和登出操作，以及运行自定义的脚本



- Login VSI是业界主流的虚拟桌面性能测试软件，主流虚拟化厂商VMware、华为、Citrix、 微软以及集成商Cisco、HP等厂商均采用该工具进行VM密度及体验测试，并以此结果作为对外发布的性能规格指标。

中载（Medium）是Login VSI中的默认负载。

MediumNoFlash是一个基于Medium的负载，除了将Adobe Flash组件禁掉了。该负载模拟一个使用Office、IE和PDF的中等程度。一旦会话启动，中载每隔12分钟重复一次。在每次循环过程中每隔2分钟计算一次响应时间。

- 中载同时打开5个应用软件。
- 中载的打字速度是每个字符160毫秒。
- 为了模拟真实的用户，大概会有2分钟的空闲时间。
- 每次循环过程中会做以下操作：
- 打开Outlook 2007/2010，浏览10条消息。
- 打开IE浏览器，一个是打开（BBC.co.uk），另一个是打开Wired.com，Lonelyplanet.com。
- 打开gettheglass.com的flash程序（在MediumNoFlash中不可用）。

LoginVSI虚拟机密度的验收标准

Activity (RowName)	Result (ms)	Weight (%)	Weighted Result (ms)
Refresh document (RFS)	160	100%	160
Start Word with new doc (LOAD)	1400	50%	700
File Open Dialogue (OPEN)	350	100%	350
Start Notepad (NOTEPAD)	50	100%	50
Print Dialogue (PRINT)	220	100%	220
Replace Dialogue (FIND)	10	500%	50
Zip documents (ZIP)	130	100%	130
	VSImax Classic Response Time		**1660**

验收标准：7个关键操作响应时间权重加权累加值,VSI 平均响应时间超过4s则判定为不可接受。

 Page 24



- 关键操作确定VSIMAX值：
  - 从home驱动盘的文档池中拷贝一个新的文档；
  - 在Microsoft中打开一个文档；
  - 打开 “File Open”对话框；
  - 启动 “Notepad”；
  - 启动 “Print”对话框；
  - 启动 “Search and Replace”对话框；
  - 用7-zip的命令行将一个文档压缩成zip文件；

- 核心思想：以连续稳定地出现高于既定标准的反馈时间为依据来判定VM的性能下滑，进而确定BenchMark值。

虚拟桌面密度测试方法二：QoE

第一步：确定用户体验基线

测试项	测试子项	酷睿 I3	酷睿 I5	权重
win Operation	鼠标移动时间	0.17	0.16	10%
	窗口切换时间	0.30	1.12	5%
Office操作	Excel打开(86K)	4.28	2.84	10%
	PPT打开(0.97M)	4.16	1.84	10%
	Word打开（2.77M）	4.96	2.73	5%
	Word打开（15M）	32.53	11.97	5%
编译	JAVA编译（eclipse）	NA	33.49	10%
	C/C++编译（VC2008）	NA	18.72	10%
日常操作	IE打开（W3首页）	1.55	1.13	5%
	小文件拷贝(总量1G)	138.17	99.76	5%
	大文件拷贝(总量1G)	19.12	16.27	5%
	解压缩(516M)	33.79	17.36	5%
	压缩(502M)	458.47	218.47	5%
音频	Espace（时延：800ms，MOS：2.8）	满足	满足	10%

 Page 25



- PC 酷睿i3配置：1.6GHz双核，2G内存，
- PC 酷睿i5配置：3.0GHz双核，4G内存

虚拟桌面密度测试方法二：QoE

第二步：QoE加压确定虚拟机密度

- 在一台服务器上运行的虚拟机数量从小到大的递增，如20、21台依次递增,在每个虚拟机中安装测试加压软件。
- 启动一定比例虚拟机中的加压软件对虚拟机的CPU/MEM/IO按照采集的测试模型进行模拟的加压
- 选取其中一台（未加压）的虚拟机进行用户体验测试采集如下信息用户体验。
- 虚拟机密度依次增加，当体验达到基准值时，即确定了虚拟机密度。



- PC 酷睿i3配置：1.6GHz双核，2G内存
- PC 酷睿i5配置：3.0GHz双核，4G内存

桌面云服务器数量的计算

第一步：服务器总量

根据服务器及CPU型号，用户场景（轻载、中载、重载）确认VM密度。比如E6000(2*E2630)**刀片服务器中载的缺省VM密度是37个**。那么500用户需要刀片数=500/37=14，再加上两个管理刀片，一块冗余保护的刀片。***共14+2+1=17块刀片。***

第二步：内存总数

每服务器物理内存= VM密度*VM规格+8G(UVP与Domain0损耗)=37*4+8=158G。内存条有8G、16G、32G的型号，所以每刀片需要158/8=**20根8G内存条。**

第三步：其他固定配置

1、每服务器至少两300G硬盘，支持RAID0、RAID1的RAID卡。

2、至少4个GE口（两个用于业务+管理，两个用于IPSAN存储）；或2个GE口+2个FC-HBA口(用于接FC-SAN)。



存储容量规划的基础知识-1

➢磁盘的有效容量

磁盘标称容量与计算机系统的有效容量转换，磁盘的有效容量=磁盘的标称容量*1000^3/1024^3。

➢RAID5的有效容量与IOPS

RAID5有一个校验盘，写惩罚是1：4，那么N个磁盘组成RAID5的有效容量与IOPS。

有效容量=标称容量*1000^3/1024^3*(RAID组盘数-1)。

有效IOPS=(单盘标称IOPS/(1+3*写比例)* RAID组盘数

样例：

5块600G SAS盘组成RAID5，单盘SAS盘的IOPS是180， 写比例60%；那么：

有效容量=600*1000^3/1024^3 *(5-1)=2232G

有效IOPS=180/(1+3*60%)*5=321。

 Page 28



- 首先使用信息采集工具采集下面数据，包括：
  - 每用户平均读写IO数；
  - 写IO所占比例(%)；
- 根据此信息，我们即可计算存储在此模型下的IOPS。存储的有效IOPS与RAID类型、IO随机写比率相关，计算方法如下：
  - RAID10

  RAID10下，由于有镜像盘，会使1个写IO产生1个额外的镜像盘写IO。

  假设用户办公产生的随机IO中写IO所占比例为x%，那么可以计算出有效IOPS的比例为1/(1+x%)，即100/(100+x)。

  - RAID5

  对一个写IO来说，如果它落到一个数据盘D上，为了完成这次写操作，需要以下几个步骤：(1)读数据盘D（2）读校验盘P（3）写校验盘P（4）写数据盘D

  可以看到，一个写盘的IO实际产生的2个写IO和2个读IO，额外多出了3次IO；读IO不会产生额外的访盘IO操作；

  假设用户办公产生的随机IO中写IO所占比例为x%，那么可以计算出有效IOPS的比例为1/(1+3x%)，即100/(100+3x)。

存储容量的计算-基础知识-2

➢RAID10有效容量与IOPS

RAID10没有校验盘，采用条带镜像方式，写惩罚是1：2；那么N个磁盘组成RAID10的有效容量与IOPS。

有效容量=标称容量*1000^3/1024^3*RAID组盘数/2

有效IOPS=(标称IOPS/(1+1*写比例))*RAID组盘数

样例：

8块2T SAS盘组成RAID10，单盘SAS盘的IOPS是80， 写比例40%；那么：

有效容量=2000*1000^3/1024^3 *8/2=7440G

有效IOPS=80/(1+1*40%)*8=457。



完整复制桌面云存储容量的计算

通过容量和IOPS两个维度计算存储设备配置，每个600G SAS硬盘的极限IOPS为180，创建RAID5后，考虑60%写比例。每框S5500T有24块盘，分3个RAID 组，盘数分别是5块、9块、9块。每框配置1块热备盘。

单框有效IOPS=(5+9+9)*(180/(1+3*60%))=1478

单框有效容量=(4+8+8)*(600*1000^3/1024^3)=11160

➢**容量维度**

总框数=(总人数*每人数磁盘空间)/每框容量= (500*120)/11160=5.4

➢**IOPS维度**

总框数=(总人数*每人IOPS)/每框有效IOPS= (500*7)/1478=2.4

➢**总结**

结合容量和IOPS维度两个角度，需要配置5.4框，还有管理节点盘数5块，共需要硬盘5.4*24+5 = 135块。每套S5500T配置1拖4框，所以需要配置2套S5500T控制框、4个硬盘框，135块硬盘。



链接克隆桌面云存储容量的计算

➢存储计算公式

普通链接克隆存储计算方式与完整复制的存储计算方式不同，需要根据链接克隆的特点来计算，但同样也要从两个维度来考虑。

链接克隆只用于系统盘，不用于数据盘。

➢ 存储容量维度

总硬盘数 = (Roundup(总人数 / 128, 0) * 母盘大小 + 总人数 * 差分盘大小) / 每盘有效容量 * 热备盘率

注：每个母盘最大支持128个虚拟机共用。

➢ 存储IOPS维度

总硬盘数 = (总人数 * (母盘IOPS + 差分盘IOPS)) / 每盘有效IOPS * 热备盘率。

故结合容量和IOPS维度，取最多的硬盘数。

 Page 31



➢ 存储计算举例

- 设链接克隆母盘大小为40G，母盘IOPS为2，差分盘的大小5G，差分盘IOPS为3；采用300G的SAS盘，组成RAID10，则：
- 每个300G SAS盘的有效容量 = 300 / (1.024 ^ 3) * 0.5 = 139G。
- 每个SAS盘的有效IOPS = 200 / (1 + 1 * 70%) = 117。
- 注：每个SAS硬盘的极限IOPS为200
- 计算 500普通链接克隆VM需要多少硬盘数?
- 容量维度
- 总硬盘数= ((Roundup(500 / 128, 0) * 40 + 500 * 5) / 139) * 12 / 11 = 22。
- IOPS维度
- 总硬盘数= (500 * (2 + 3)) / 117 * 12 / 11 = 24。
- 故结合容量和IOPS维度，500普通链接克隆虚拟机最少需要24块300G的SAS盘。

PvD桌面云存储容量的计算

➢**存储计算公式**

PvD链接克隆存储计算方式与普通链接克隆的存储计算方式也有一点不同，但同样也要从容量与IOPS两个维度来考虑

➢**存储容量维度**

总硬盘数 = (Roundup(总人数 / 128, 0) * 母盘大小 + 总人数 * PvD盘大小) / 每盘有效容量 * 热备盘率

注1：每个母盘最大支持128个VM共用

注2：每个差分盘几乎没有写入数据，大小接近于0，忽略，不在公式中出现

➢**存储IOPS维度**

总硬盘数 = (总人数 * (母盘IOPS + PvD盘IOPS)) / 每盘有效IOPS * 热备盘率

注1：每个差分盘几乎没有写入数据，IOPS接近于0，忽略，不在公式中出现

故结合容量和IOPS维度，取最多的硬盘数。

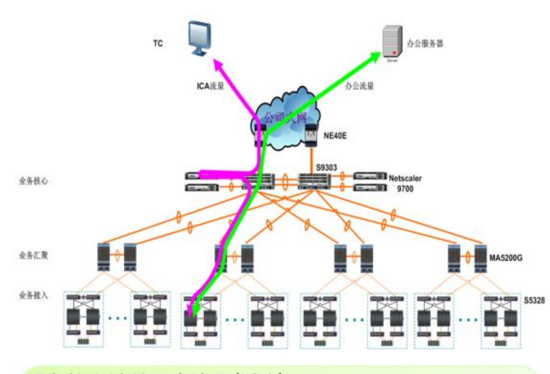
 Page 32



- **存储计算举例**
- 设链接克隆母盘大小为40G，母盘IOPS为2，PvD盘的大小10G，PvD盘IOPS为3；采用300G的SAS盘，组成RAID10，则：
- 每个300G SAS盘的有效容量 = 300 / (1.024 ^ 3) * 0.5 = 139G。
- 每个SAS盘的有效IOPS = 200 / (1 + 1 * 70%) = 117。
- 注：每个SAS硬盘的极限IOPS为200
- 计算 500PvD链接克隆ＶＭ需要多少硬盘数?
- 容量维度
- 总硬盘数= ((Roundup(500 / 128, 0) * 40 + 500 * 10) / 139) * 12 / 11 = 42。
- IOPS维度
- 总硬盘数= (500 * (2 + 3)) / 117 * 12 / 11 = 24。
- 故结合容量和IOPS维度，500PvD链接克隆虚拟机最少需要42块300G的SAS盘。

网络带宽的计算

桌面云ICA流量分析模型



统计类型	每VM到TC流量kbps	TC到VM流量kbps
静默不操作	13	0
文件夹操作	40	30
文本编辑浏览	100	15
PPT/大图片	300	15
网页浏览	100	20
eSpace语音	200	30
MP3	300	50
标清视频	2000	50
高清视频	2000~10000	80
每用户平均值	**139.4**	**21.1**

TC 接入端单用户流量(ICA)：

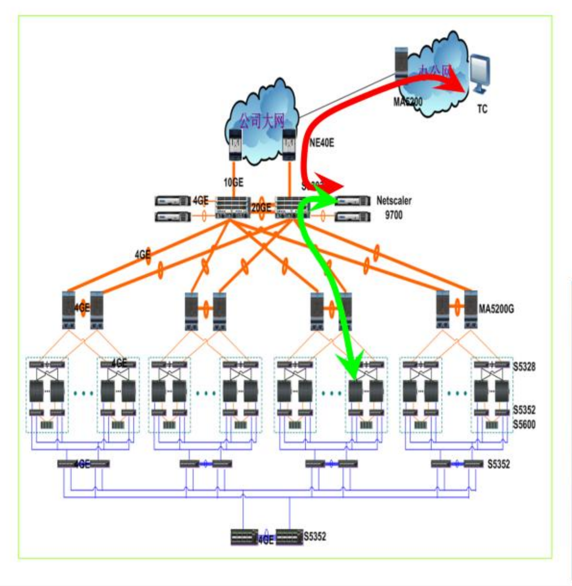
- ✓ 单用户正常办公流量：平均80k～200k;
- ✓ espace语音流量约为200K;
- ✓ 最大2～10M（高清视频播放）


ICA的占用业务带宽跟用户行为强相关

通过对网络流量的分析计算网络带宽，保证网络建设的合理性和业务连续稳定运行。
每用户平均带宽需求＝（100kbps×16%(互联网浏览)＋100kbps×80%（文档编辑）＋2000kbps×4%（视频浏览））/80%＝220kbps。

  HUAWEI

网络QoS要求



OA办公桌面的网络QoS的要求

网络质量等级	包丢失率	抖动 (ms)	单向时延 (ms)
良好 （办公要求）	≤0.1%	≤5	≤25
一般	0.1%～1%	5～20	25～50
较差	1%～5%	20～60	50～200
特别差	≥5%	≥60	≥200

- **桌面云数据中心内部通过以下方式保证QoS：**

二层网络启用802.1P，进行流分类，标识出ICA流量；
启用PQ队列调度，避免拥塞，优先转发ICA流量；

- **传输网络需要启用区分服务保证QoS：**

根据RDP/ICA的优先级表示，进行不同的DSCP标记，设置为EF或者AF级别，进行优先转发，保证网络拥塞后的RDP/ICA流量优先转发；

- **对于TC接入网络，做类似处理，保证接入侧优先级：**

二层网络启用802.1P和PQ队列；
三层接入部分采用DSCP区分服务；



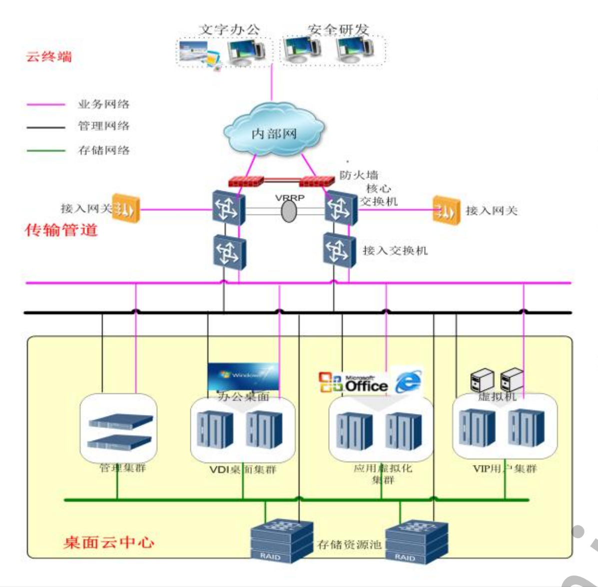


 Page 35



- 容量规划的三个方面：服务器的容量、存储的容量、网络带宽的容量

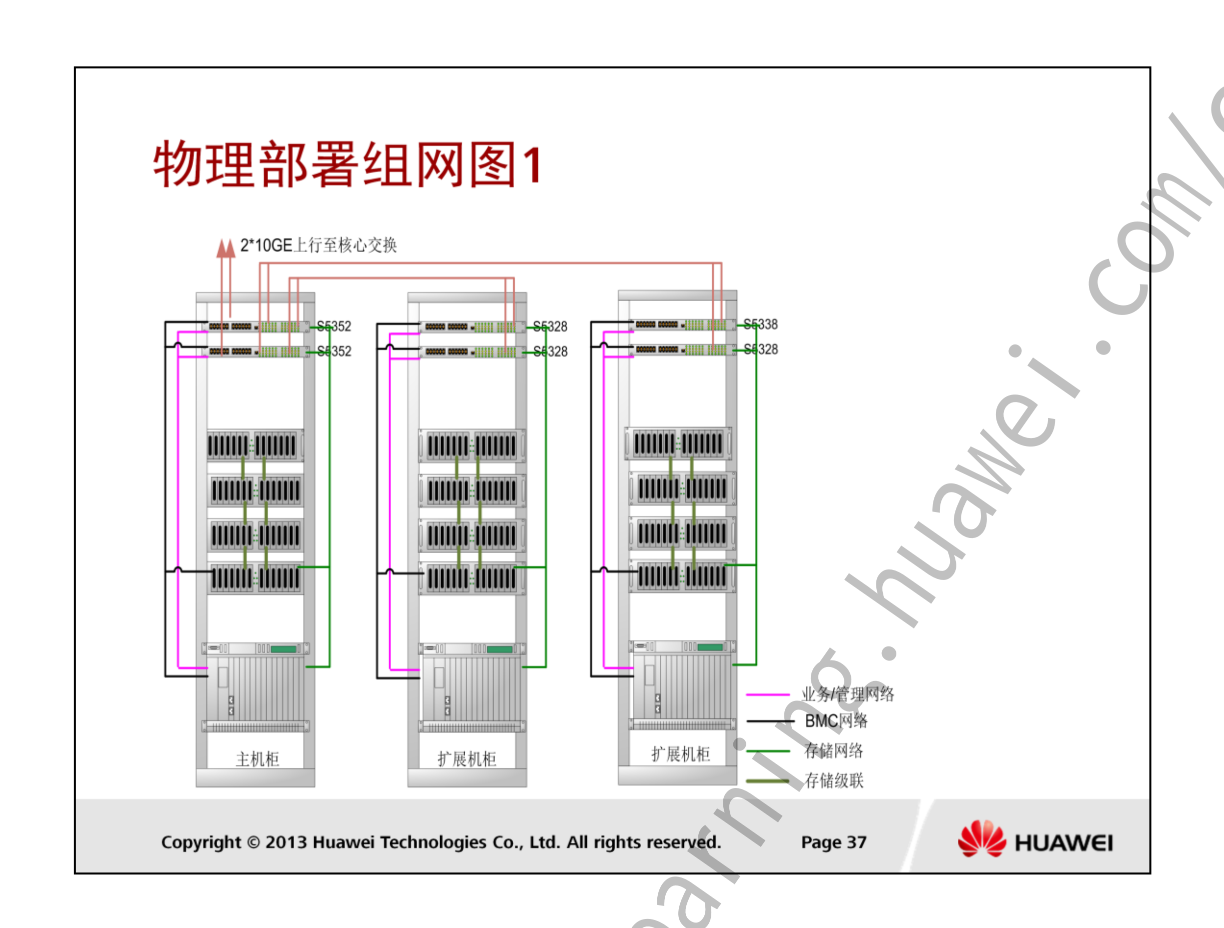
逻辑组网图



组网要点

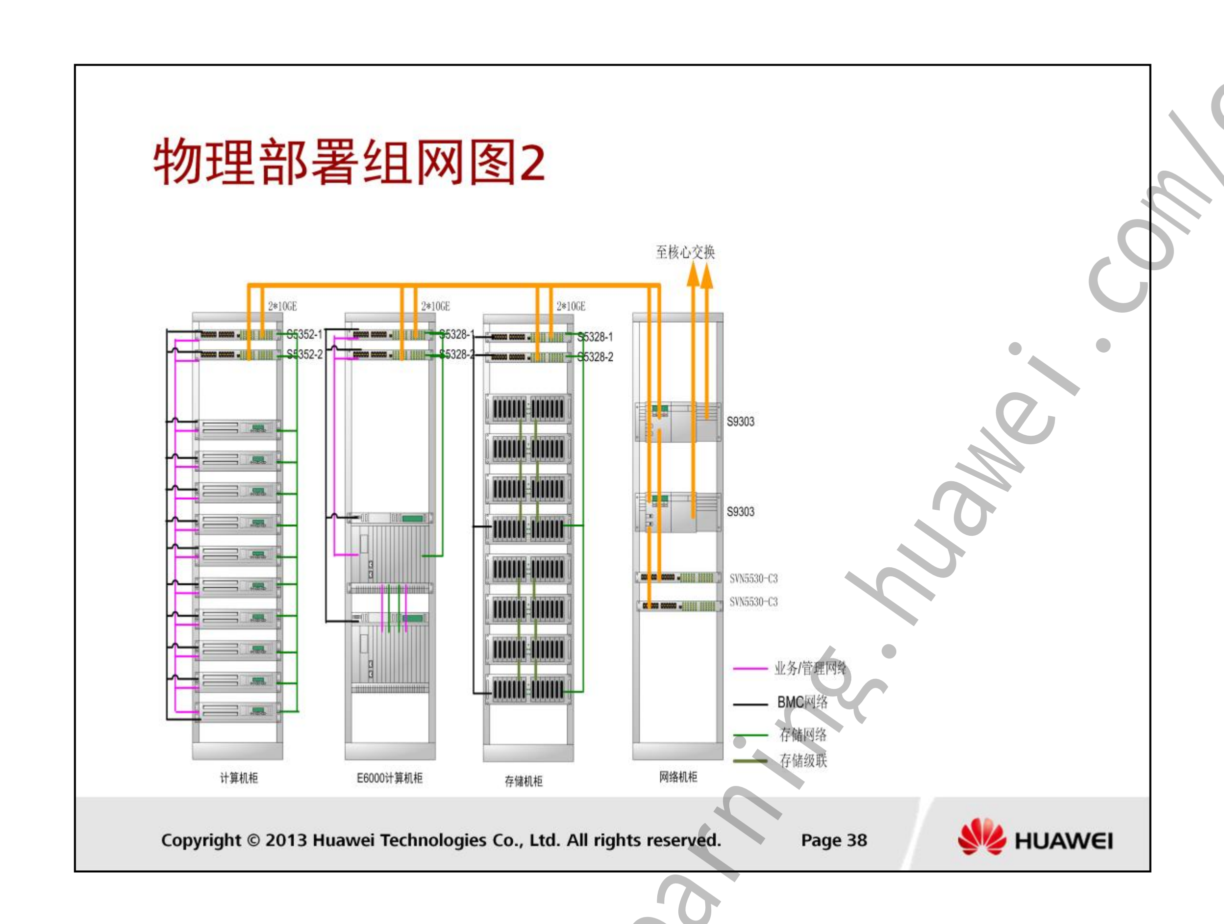
- 云、管、端三位一体；
- 业务网、管理网、存储网三网隔离；
- 全网双平面上行连接，交换机采用SmartLink上行，避免单点故障；
- 接入网关旁挂，并且VRRP冗余组网，保障安全可靠。





组网要点

- 采用刀片服务器+SAN的组合，一般每机柜一框刀片+一套存储。
- 网络一般采用两层设计，扩展机柜的交换柜内接入交换机都接到主机柜。主机柜直接上行到核心交换机。
- 机柜数量比较少时，建议采用，级联到6个机柜。



组网要点

- 一般服务器、存储、网络设备单独组柜。
- 网络一般采用三层设计、柜内接入交换机、汇聚交换机、汇聚交换机再上行到核心交换机。
- 机柜数比较多时，多于6个机柜，建议采用这种方式。

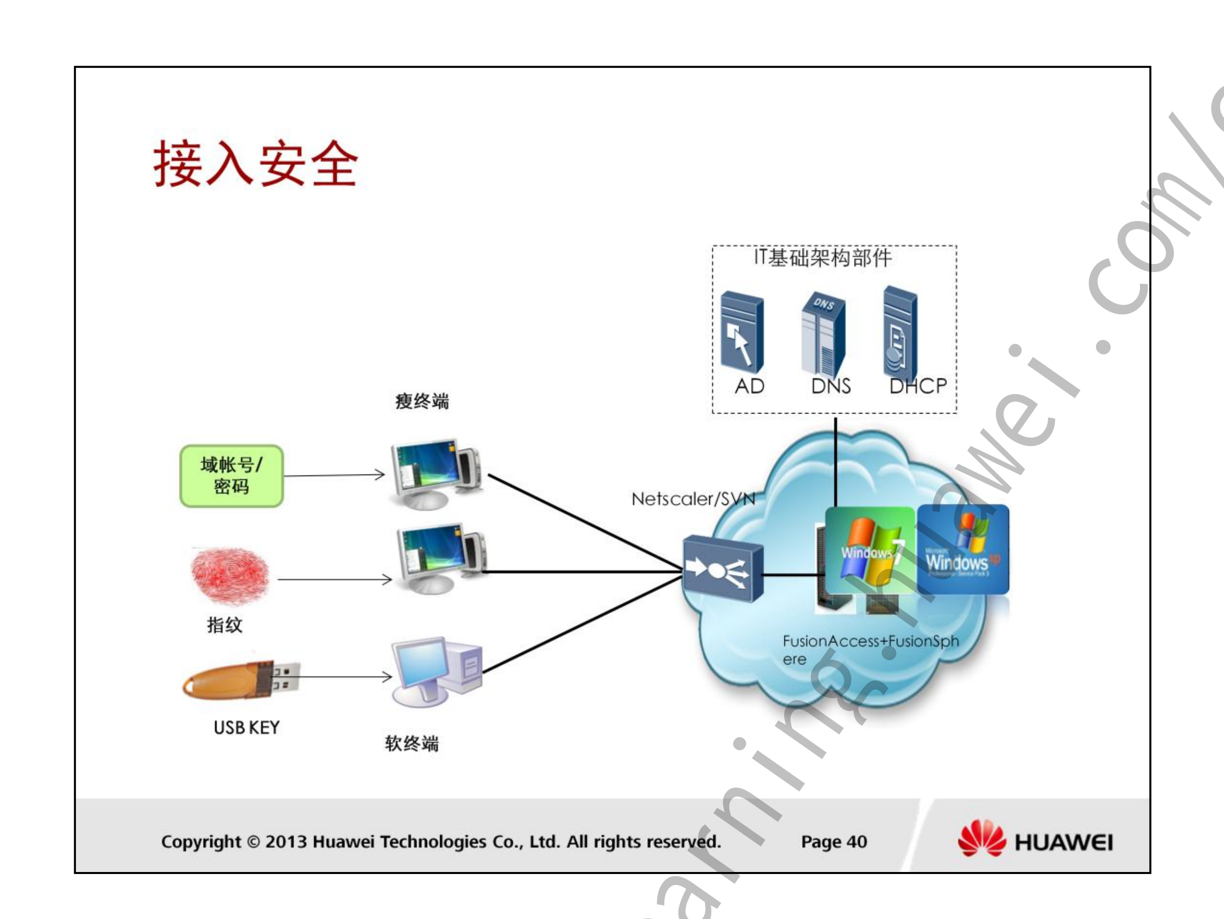


目录

 Page 39



- 容量规划的三个方面：服务器的容量、存储的容量、网络带宽的容量



方案要点

- 用户身份认证方式，AD域密码、指纹认证、动态口令认证、USB KEY认证。
- 是否需要接入网关/负载均衡器。
- TC的配置（根据外设类型、应用场景类型配置TC）。

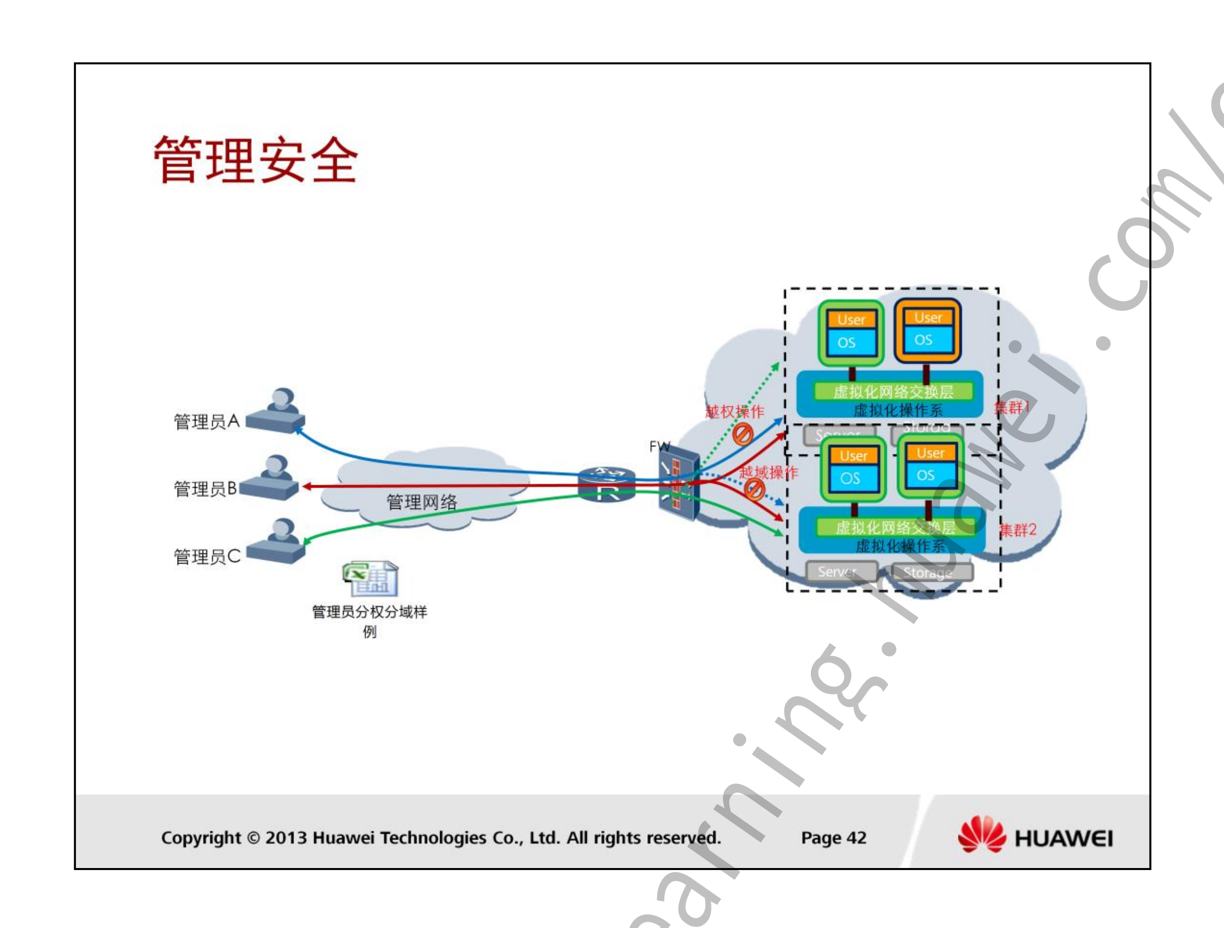
网络隔离，安全域划分

Untrust域
云终端
防火墙
DMZ域
负载均衡器
Base域
基础服务虚拟机
NTP
WSUS
AD/DNS/DHCP
OMM域
云管理虚机
FusionManager
FusionCompute
VDI域
桌面管理虚拟机
DDC
WI
TCM
ITA
User域
用户虚拟机
VM
VM
VM
VM
硬件

HUAWEI

网络隔离要点

- **集群隔离：** 按照用户群，应用类型，划分服务器集群，服务器可以做到物理隔离隔离。
- **VLAN隔离：** 各部门的虚机，各管理节点，基础服务虚机划分不同VLAN进行逻辑隔离。
- **安全域隔离：** 防火墙安全域的按客户要求划分，配置访问策略。缺省划分为Untrust域、DMZ域、Base域、OMM域、VDI域、User域。在防火墙上配置相应的访问策略。 USER域根据客户要求进一步再细分。



管理安全系统缺省具体的安全，最重要的就是管理员的权限的限制，创建管理员时注意分权分域的配置。遵循NIST标准模型，支持灵活的创建角色和管理员，使得管理员不能越权管理。

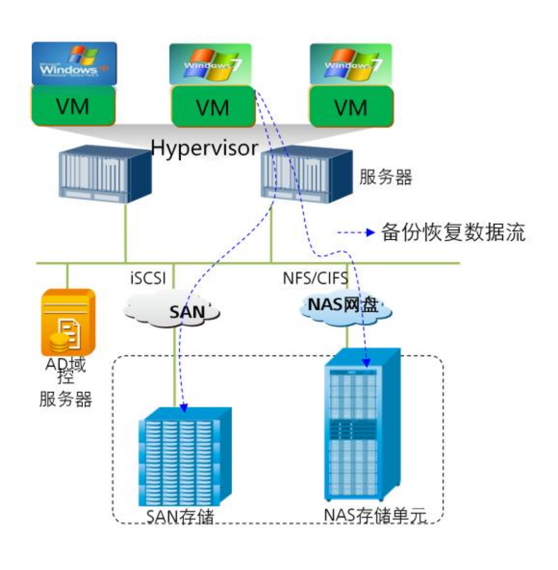
- “分权”：区分操作权限，由“角色”进行控制。一个“角色”可拥有一个或多个不同的“操作权限”，一个“用户”可拥有一个或多个不同的“角色”。通过绑定“用户”和“角色”，实现“用户”和“操作权限”的绑定。
- “分域”：区分管理的数据权限，也即管理员能够管理的范围，如“管理员A”仅能管理“集群1”中虚拟机，“管理员C”仅能管理“集群2”中虚拟机。



目录



数据备份方案一：NAS备份

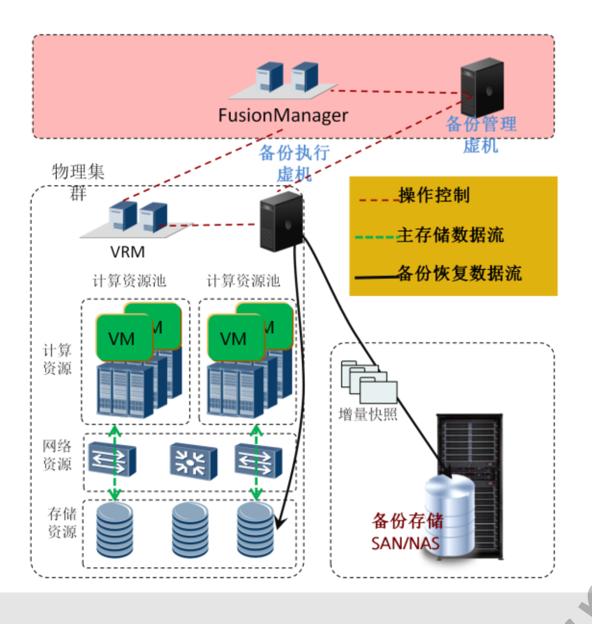


方案要点

- **方便快捷**：用户直接采用Windows系统自带备份恢复即可。用户可自行选择备份目录与文件，自行恢复。
- **组网简捷**：增加一个NAS设备即可，可考虑文件服务器，N2000，或N8000。



数据备份方案二：虚拟机快照备份



➢HyperDP系统

基于华为虚拟化平台自研虚拟机快照备份系统,管理员接入DPS的备份管理系统进行备份保护，支持对系统卷与数据卷的快照备份。

主要包括

➢备份管理服务器(Dispatcher DPS)：

备份和恢复任务操作转发，从备份服务器(Processor)管理。备份和恢复任务管理界面呈现。

➢备份服务器(Processor DPS)

备份任务和恢复任务管理，虚拟机备份和恢复。

 Page 45



- 备份系统对虚机卷（包括系统卷和/或数据卷）数据进行备份，不需要终端用户参与，也不需要在VM里安装代理，且不影响生产系统的运行；当生产系统由于意外丢失VM卷数据时，系统管理员可以通过本地备份系统恢复VM卷数据，以保证VM能继续正常工作。管理员接入DPS的备份管理系统进行备份保护，支持对系统卷与数据卷的快照备份。其功能包括：
- 备份管理系统可以进行虚拟机卷备份策略灵活设置，选择需要备份的虚机，备份起始时间、配置全量备份和增量备份的周期。
- 虚拟机备份执行：备份管理在执行备份策略，调用VRM接口生成虚机的全量快照与增量快照，然后复制快照到本地存储或NAS上保存。
- 虚拟机备份信息查询：可以查询指定虚机在NAS或本地存储上的历史虚拟机备份信息。
- 虚拟机备份文件删除：可以根据备份保留策略对备份目录中保存的备份文件进行删除。
- 根据备份文件恢复虚机：可以从NAS或本地存储读取快照文件恢复虚拟机。管理员可以选择恢复到原有虚机、或者新虚机、或者其它虚机。

备份策略设计

备份策略：由业务系统的重要性和数据量来决定，备份作业运行频率，启动时间。

例

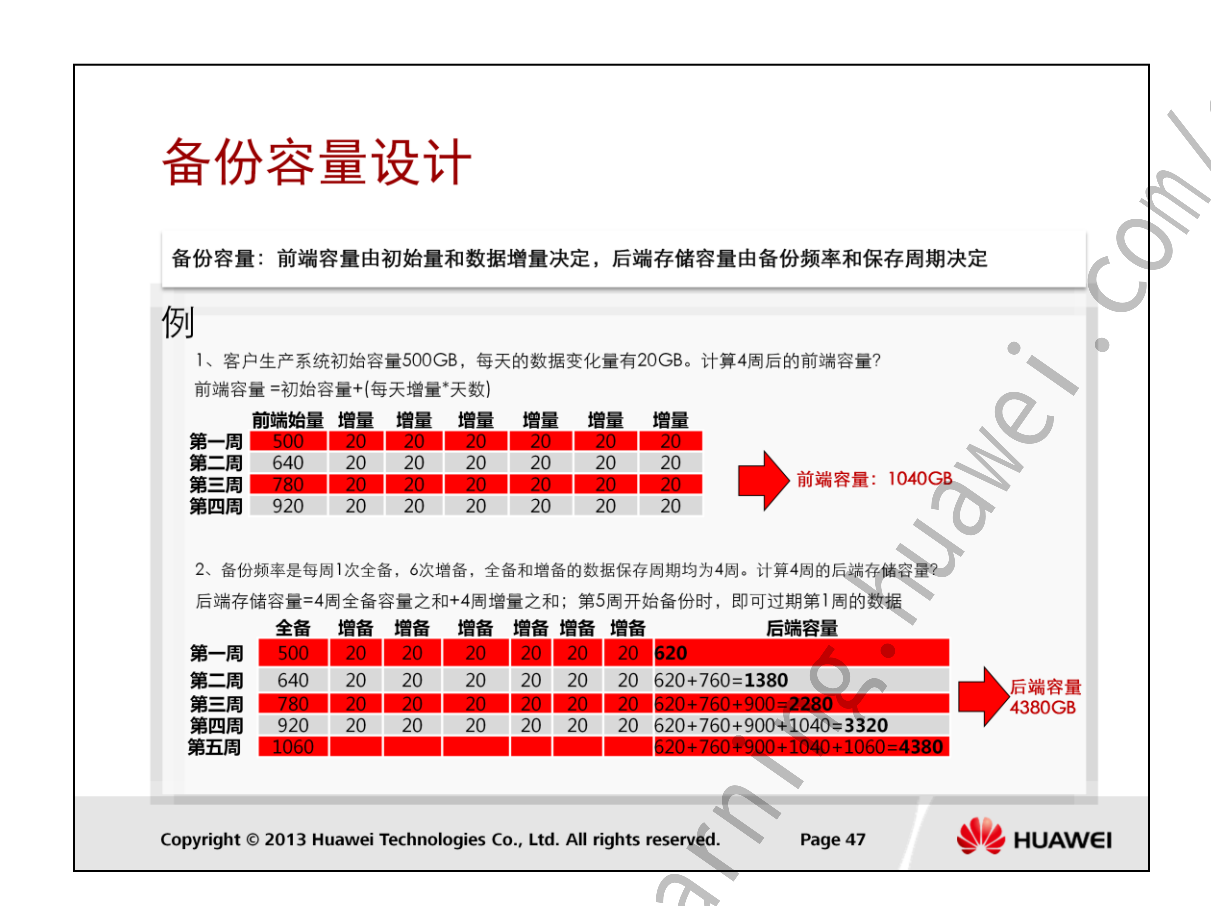
业务子系统		备份策略	
重要性	数据量	备份类型	保留周期
高	多(eg:>500GB)	每周1次全备 每天1次增备	保留6个月
高	少(eg:<100GB)	每3小时1次全备	保留6个月
较高	少 (eg:<100GB)	每天1次全备	保留3个月
一般	一般(eg:<500G)	每两周1次全备 每天1次增备	保留2个月

注 上表为建议值，备份策略可根据客户需求配置

 Page 46



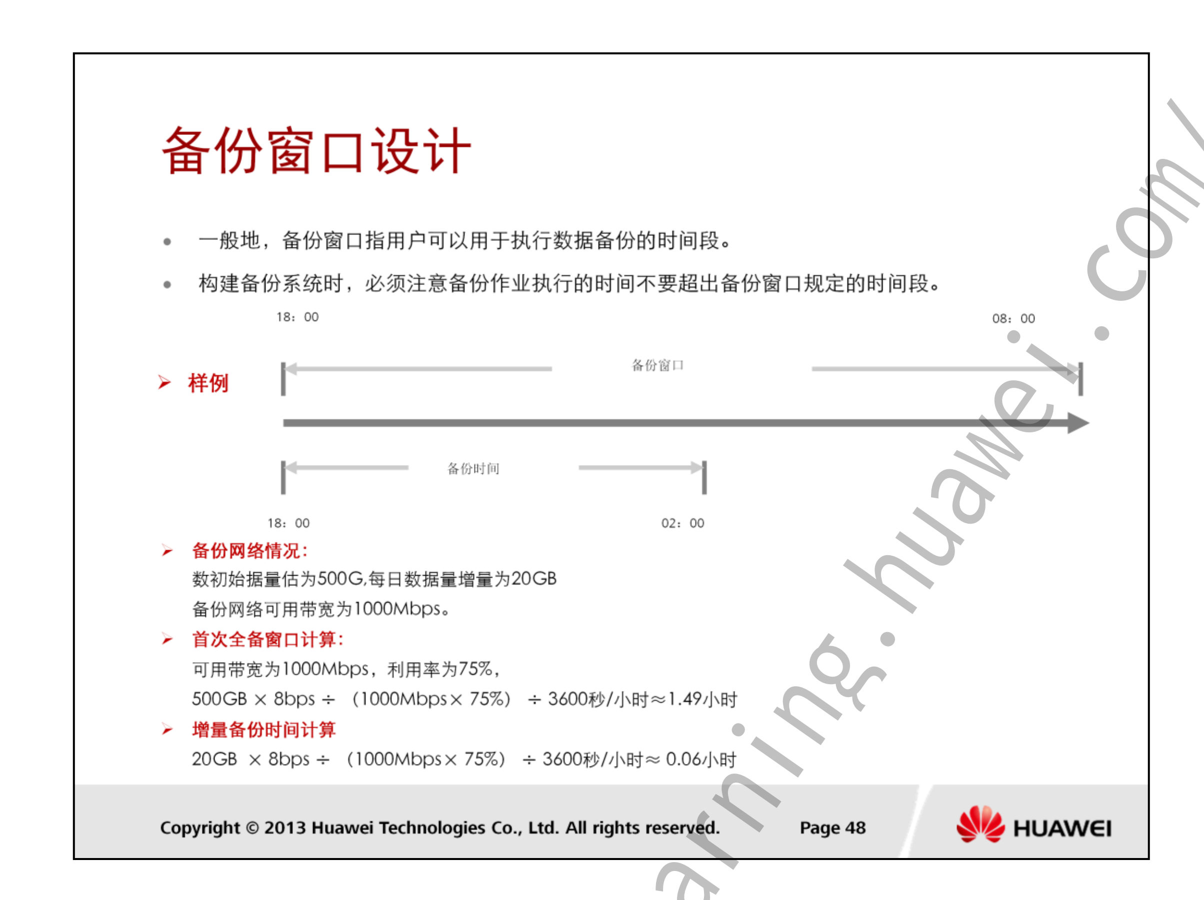
- 备份策略：由业务系统的重要性和数据量来决定，备份作业运行频率，启动时间。



	前端始量	增量	增量	增量	增量	增量	增量
第一周	500	20	20	20	20	20	20
第二周	640	20	20	20	20	20	20
第三周	780	20	20	20	20	20	20
第四周	920	20	20	20	20	20	20

	全备	增备	增备	增备	增备	增备	增备	后端容量
第一周	500	20	20	20	20	20	20	**620**
第二周	640	20	20	20	20	20	20	620+760=**1380**
第三周	780	20	20	20	20	20	20	620+760+900=**2280**
第四周	920	20	20	20	20	20	20	620+760+900+1040=**3320**
第五周	1060							620+760+900+1040+1060=**4380**

- 备份容量：前端容量由初始量和数据增量决定，后端存储容量由备份频率和保存周期决定。这里主要是指 备份的后端容量。



- 主要是指主存储到备份存储的备份网络带宽，备份时间需要多长。

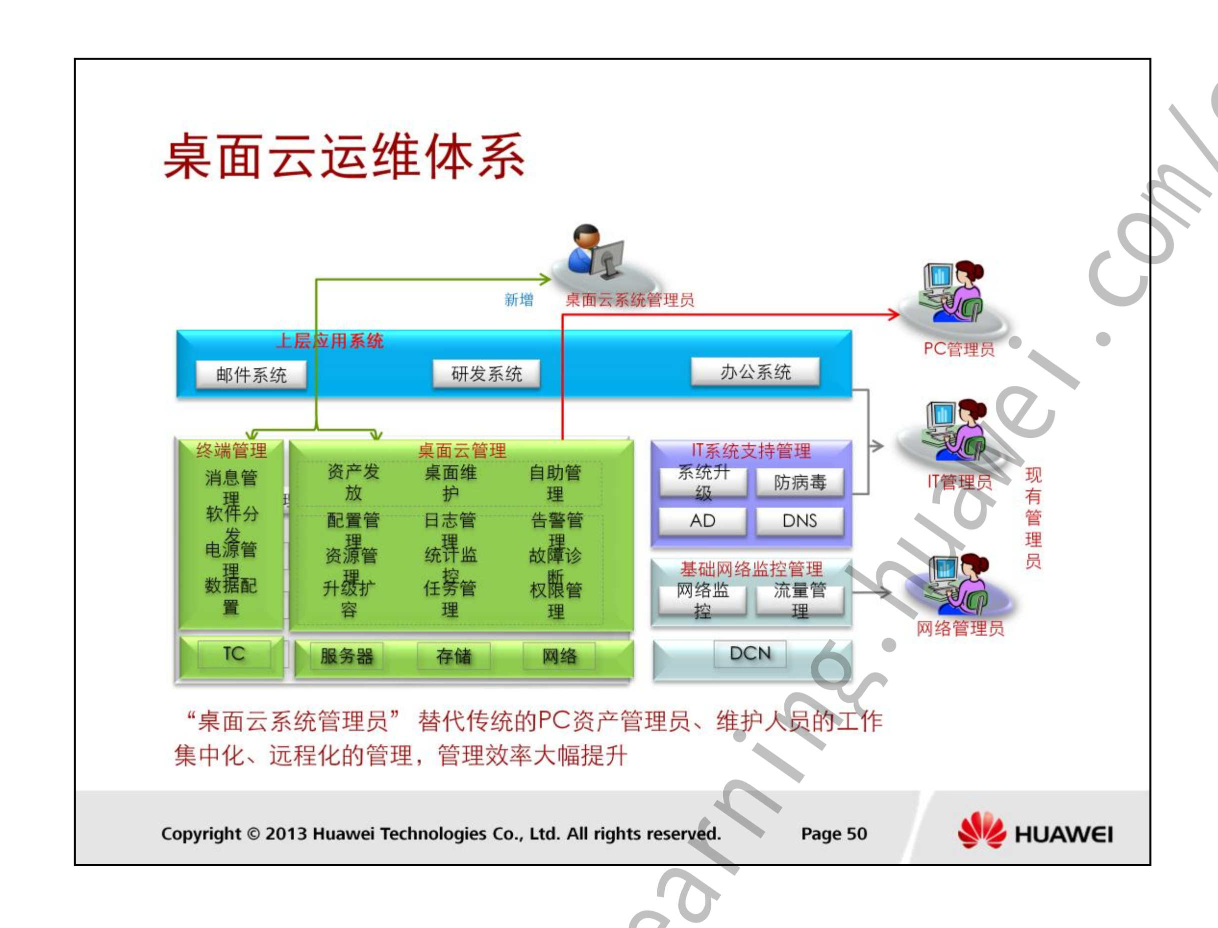


目录

 Page 49

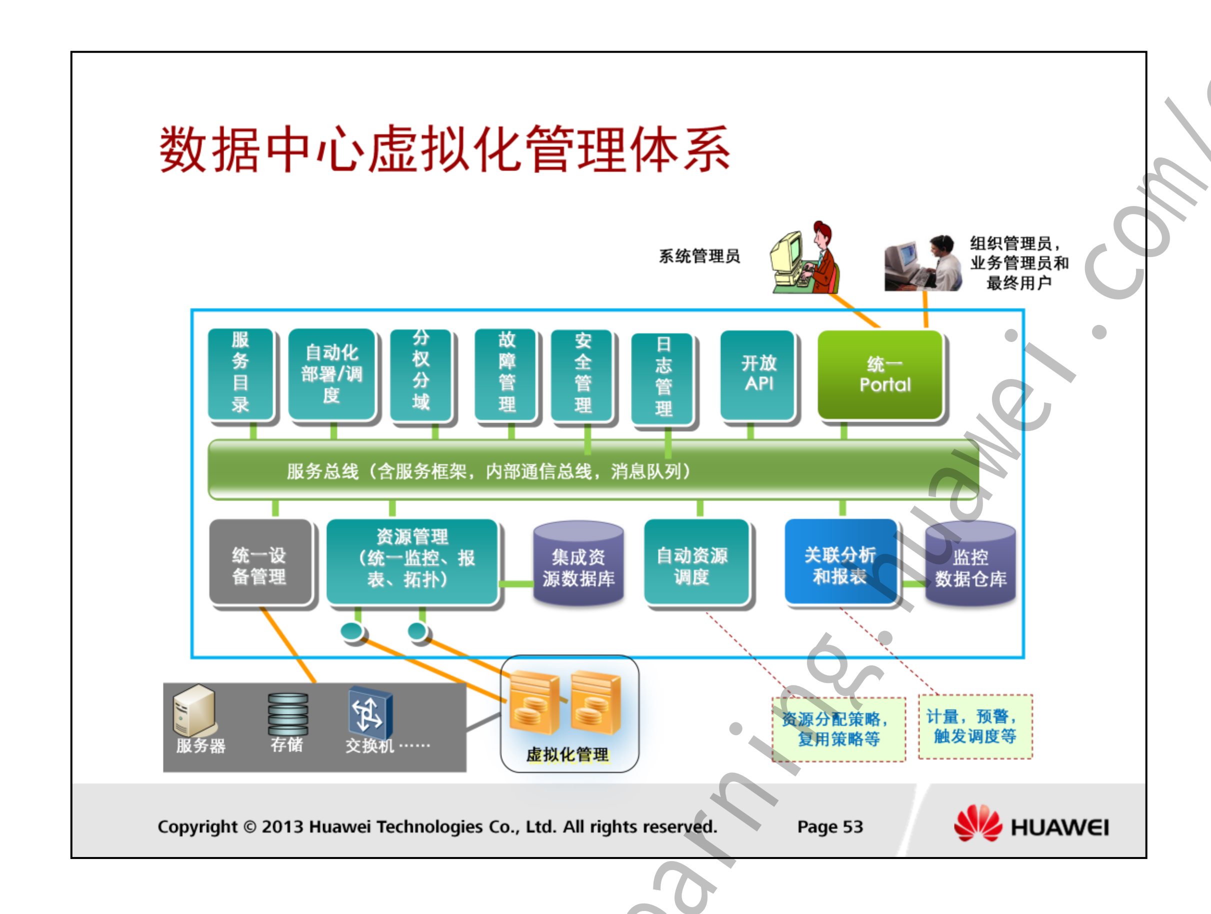


- 容量规划的三个方面： 服务器的容量、 存储的容量、网络带宽的容量



- 现有管理员：IT管理员，网络管理员，PC管理员。切换到桌面云后，PC管理员可以撤换，增加桌面云管理员，或者让IT管理员充当桌面云管理员。
- 华为桌面云运维服务管理，基于B/S架构，提供远程集中运维管理，全中文界面。华为运维管理参考ITIL标准，基于统一维护，可运营、可管理的理念，设计了符合虚拟化产品特点，易运维的管理系统。支持友好的WebUI维护界面，统一管理所有硬件资源与虚拟化资源，VDI桌面，提供基于定制化策略的自动化运维系统。
- 华为FusionAccess的统一资源发放WEB PORTAL，业务发放更灵活、更高效。强大的OM运维能力，支持用户分权分域管理，安全性高。管理员可通过Portal快速地进行业务发放、桌面管理、模板管理、权限管理、资源管理、监控管理、告警管理、拓扑管理、日志管理、任务管理、统计管理。
- 管理员登录支持SSL、数据加密、用户密码加密保存，确保用户数据安全。
- 桌面管理支持虚拟桌面生命周期管理、快照、使用快照创建虚拟机和恢复虚拟机。为用户数据提供备份功能。
- 拓扑管理能让管理员非常直观地看到系统的部署情况、运行情况。
- 告警管理支持告警转E-Mail、短信的即时通知，使用户及时了解系统。
- 日志管理支持操作日志、运行日志记录，便于审计和故障处理。FusionAccess支持集中日志，用户桌面日志、管理日志进行集中收集和分析；


基于WEB的可视化运维管理
云平台运维
硬件资源管理
多集群管理
虚拟资源管理
统一监控
第三方设备
桌面云运营
业务发放
多域管理
生命周期
定时任务
终端管理
消息通知
远程协助
补丁任务
版本升级
固件刷新
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 52
HUAWEI

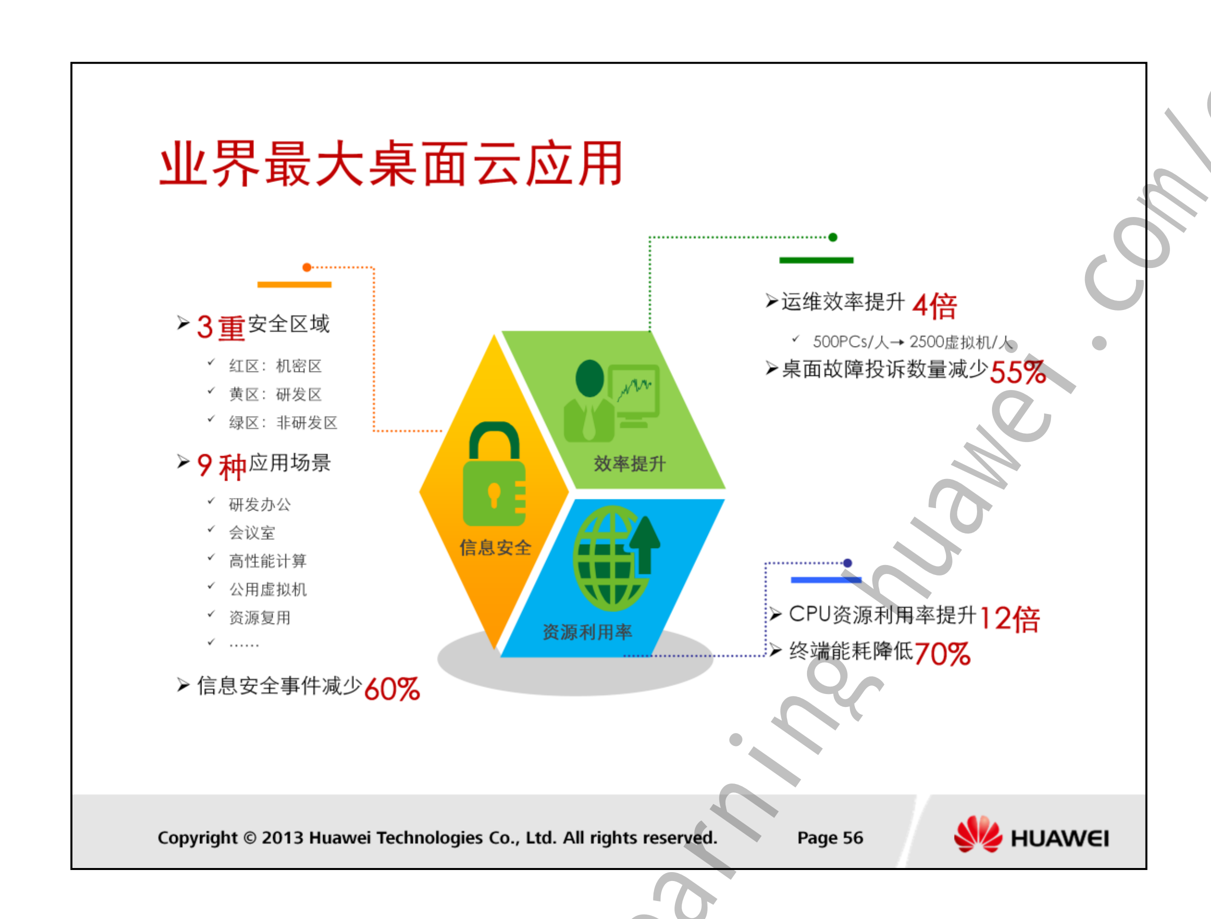


- 方框内是FusionManager云管理平台的功能模块。“虚拟化管理”可以采用华为的虚拟化管理软件FusionCompute，也可以采用其他厂家的，如VMware的VCenter+Vsphere等
- 云管理软件从软件层面拉通统一各资源管理。
- 现有管理员：IT管理员，网络管理员。IT管理员可以在维护管理Portal进行虚拟机管理，调度部署，监控，拓扑等统一管理。
- 资源管理--物理设备管理--以设备树展现一体机内部硬件组成，查询各硬件基本信息、硬件规格、实时状态、实时和历史监控指标、告警信息。提供硬件基本维护操作。
- 资源管理--资源池管理
- 资源管理-资源集群管理
- 资源管理-虚拟机管理：虚拟机基本信息查询，实时、历史监控指标查询，告警统计，虚拟机操作：启动、关闭、重启、休眠、迁移、VNC登录、修复虚拟机、虚拟机快照，下电时修改虚拟机硬件（CPU、内存、网卡、硬盘）配置。
- 告警管理：告警系统支持一体机解决方案如下部件的管理，即支持告警的管理，同时也支持第三方部件的管理，SVN和NetScaler部件的告警管理。管理员需要定期查看告警窗口是否存在告警，根据告警处理帮助消除告警。
- 拓扑视图可以查看物理硬件资源视图，应用部署以及虚拟机资源视图。



HUAWEI


华为公司内部研发全面部署桌面云
建设驱动力
信息安全：数据信息不再存储在PC终端，集中管理，保护核心技术资产
提升效率：提升设备CPU利用率，缩短办公设备部署时间，提升IT维护人员效率
灵活环保：降低办公终端设备能耗，打造低噪音、低辐射、低散热的办公环境
建设历程
2008：启动桌面云研发
2009：内部小范围试点，部署300用户
2010：启动一期项目，上海研究所率先规模部署，用户数达到7300
2011：启动二期项目，总部D/H区、北京研究所、13个海外代表处完成部署，用户规模达到3万人
2012：南研、杭研、武研、成研、西研等其余国内外研究所全面覆盖，全公司完成7万用户桌面云部署
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 55
HUAWEI



- 详细参见《华为FusionCloud 桌面云解决方案最佳实践》
- http://3ms.huawei.com/mm/docMaintain/mmMaintain.do?method=showMMDetail&f_id=DC13031337370097



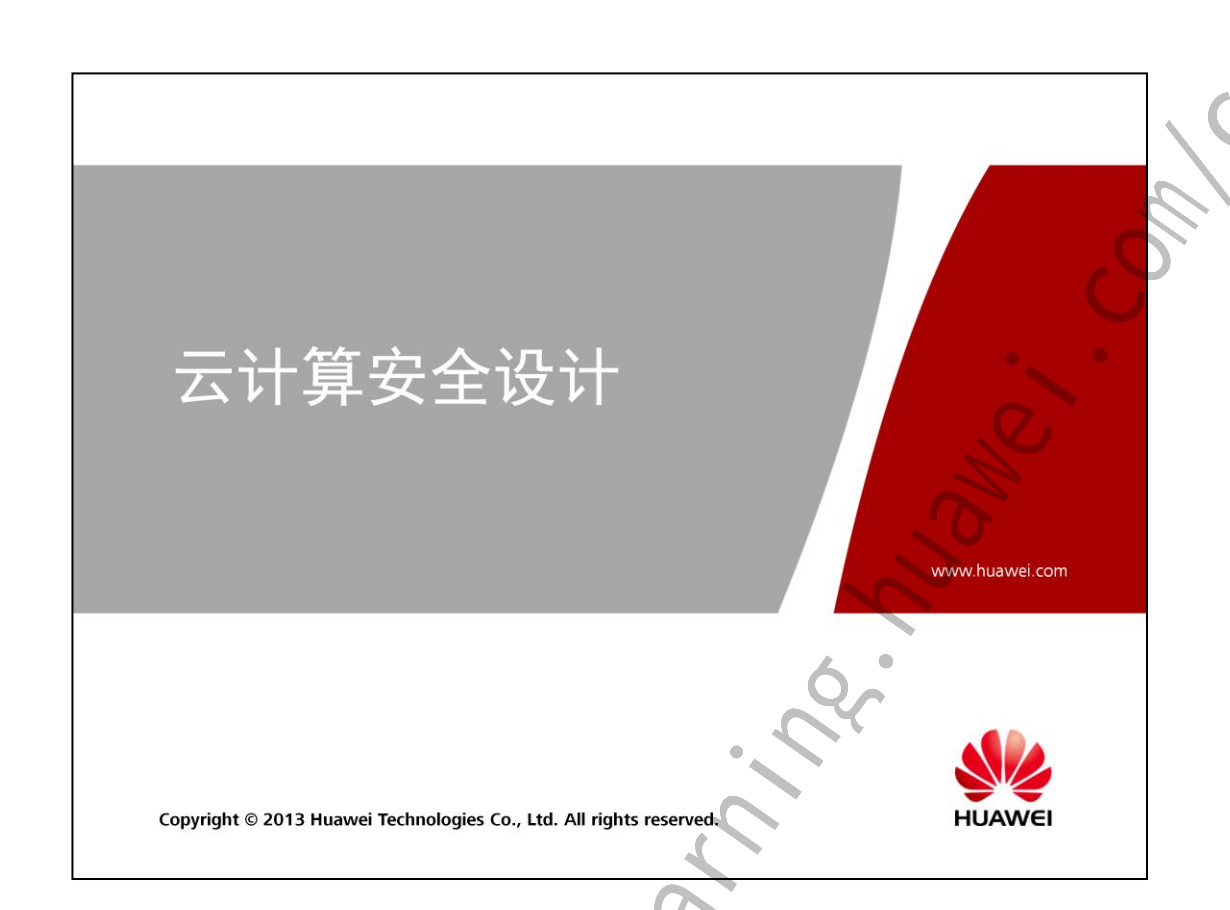
总结

- 桌面云适用的场景与需求分析；
- 数据中心虚拟化的场景与需求分析；
- 按项目的需求分析写出对应的技术建议书；
- 技术建议书各个章节、并能独立写作；
- 桌面云的容量规划与配置；
- 服务器虚拟化的容量规划与配置；



Thank you

www.huawei.com


云计算安全设计
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

- 学完本课程后，您将能够:
  - 了解云安全基本知识
  - 了解终端及接入安全
  - 了解网络安全
  - 了解虚拟化软件安全
  - 了解数据安全
  - 了解运维安全
  - 了解基础设施安全

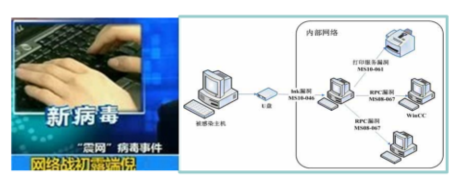


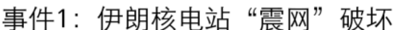


目录



信息安全形势日益严峻




事件1：伊朗核电站“震网”破坏

震网病毒（Stuxnet），是世界上首个以直接破坏现实世界中工业基础设施为目标的蠕虫病毒，被称为网络“超级武器”。震网病毒于2010年7月开始爆发，通过USB接口传染。据统计，目前全球已有约45000个网络被该病毒感染，其中60%的受害主机位于伊朗境内，并造成伊朗核电站推迟发电


事件2：高通CEO便携丢失

2001年5月，高通公司CEO欧文雅各布斯不慎在一次会议中**丢失了他的便携机**。失踪的电脑是雅各布斯用作“商业”用途的，上面存有机密信息，引发了高通公司的股价在随后的几个月内出现了较大振荡

以破坏系统运行或者窃取机密信息为目的的信息安全事件频发

 Page 4



“震网”(Stuxnet)是一种计算机蠕虫，专门针对工业巨擘西门子生产的监控和数据采集系统(SIMATIC WINCC)。只要电脑操作员将被病毒感染的U盘插入USB接口，这种病毒就会在不需要任何操作的情况下，取得工业用电脑系统控制权。 这是全球第一种投入实战的“网络武器”，它的打击对象或许就是饱受西方谴责的伊朗布舍尔核电站。

2010年7月25日，“维基解密”通过英国《卫报》、德国《明镜》和美国《纽约时报》公布了92000份美军有关阿富汗战争的军事机密文件。10月23日，“维基解密”公布了391,832份美军关于伊拉克战争的机密文件。11月28日，维基解密网站泄露了25万份美国驻外使馆发给美国国务院的秘密文传电报。“维基解密”是美国乃至世界历史上最大规模的一次泄密事件，其波及范围之广，涉及文件之众，均史无前例。该事件引起了世界各国政府对信息安全工作的重视和反思。据美国有线电视新闻网12月13日报道，为防止军事机密泄露，美国军方已下令禁止全军使用USB存储器、CD光盘等移动存储介质。

2001年5月，高通公司的CEO欧文雅各布斯不慎在一次会议中丢失了他的便携机。由于上面存有机密信息，高通公司的股价在随后的几个月内出现了较大振荡。

美国高通公司首席执行官欧文·雅各布斯１７日在参加一次演讲中丢失了自己的笔记本电脑，而这个电脑中存有“很有价值的”机密。当天，雅各布斯应邀为美国商业编辑与作家协会的成员演讲，演讲结束后有人单独向他提问，他就将自己用来作幻灯片演示的电脑放在一边的桌子上。大约１５到２０分钟后，他发现自己的电脑已经不翼而飞。

高通公司发言人克里斯蒂娜·特林布尔说，失踪的电脑是雅各布斯用作“商业”用途的，大约价值４０００美元，设有密码保护，其中的数据在他办公室的另外一台电脑中有备份。事实上，使用视窗操作系统的电脑即使有密码也很容易被破解。雅各布斯为此非常烦恼，甚至考虑过要请联邦调查局协助调查。

信息安全呼唤新的安全架构



1、PC已部署铁桶般的防御还防不住泄密?

2、内外部的威胁如何通过技术+管理的手段有效防范?

3、如何提升安全效率?提高安全投入产出比?



基于云的安全架构

改变 提升安全水平

终端简化，数据集中

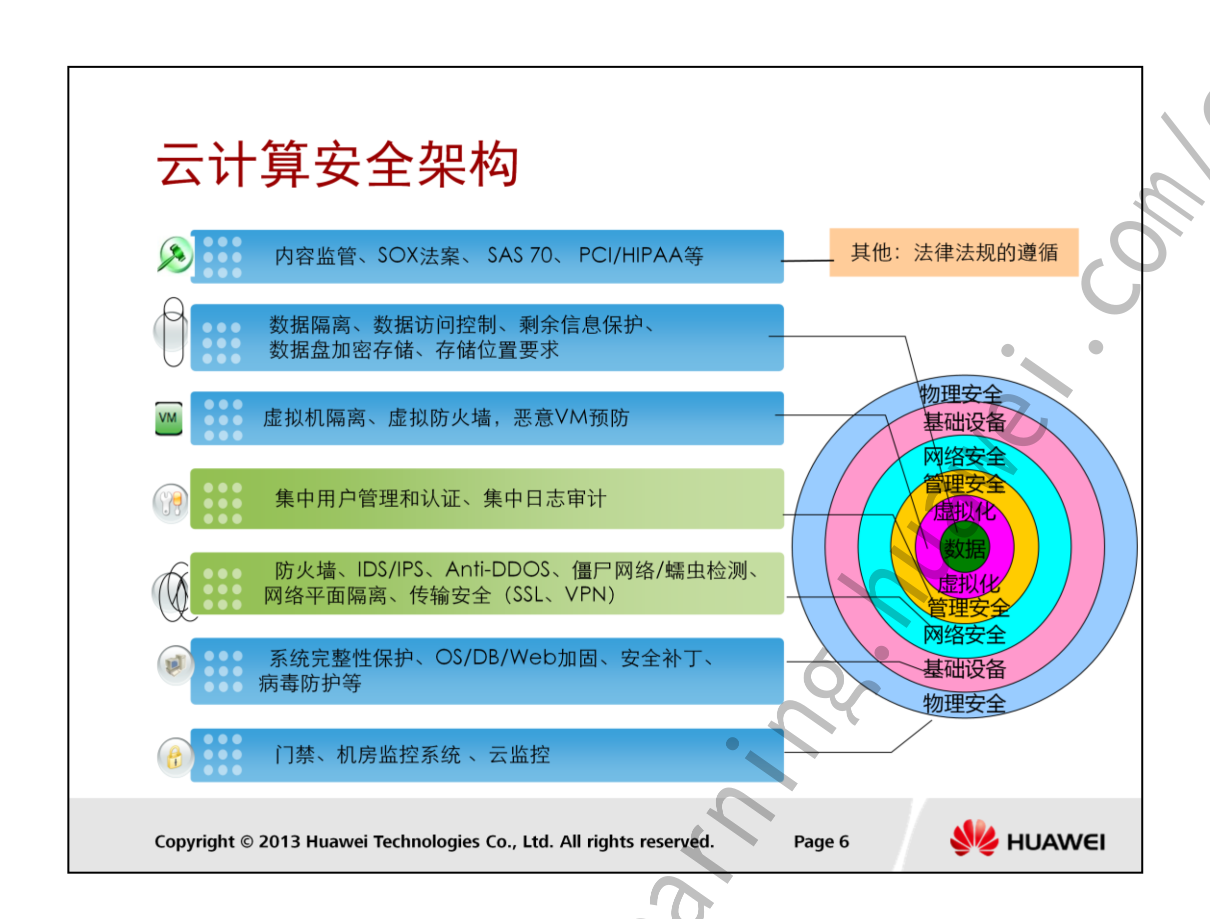
先进架构：云架构

安全资源和能力集中



终端云化，数据集中，安全资源集中，打造基于云的安全架构

HUAWEI



- 简单过一下：说明，全方位考虑了安全



目录

1. 云安全基本知识
2. **终端及接入安全**
3. 网络安全
4. 虚拟化软件安全
5. 数据安全
6. 运维安全
7. 基础设施安全



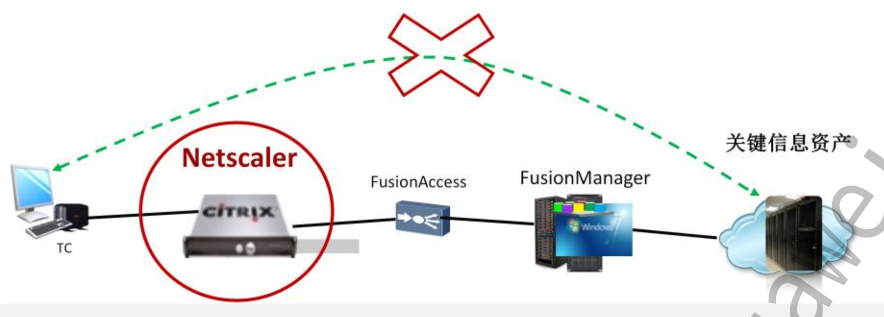


目录

2. 终端及接入安全

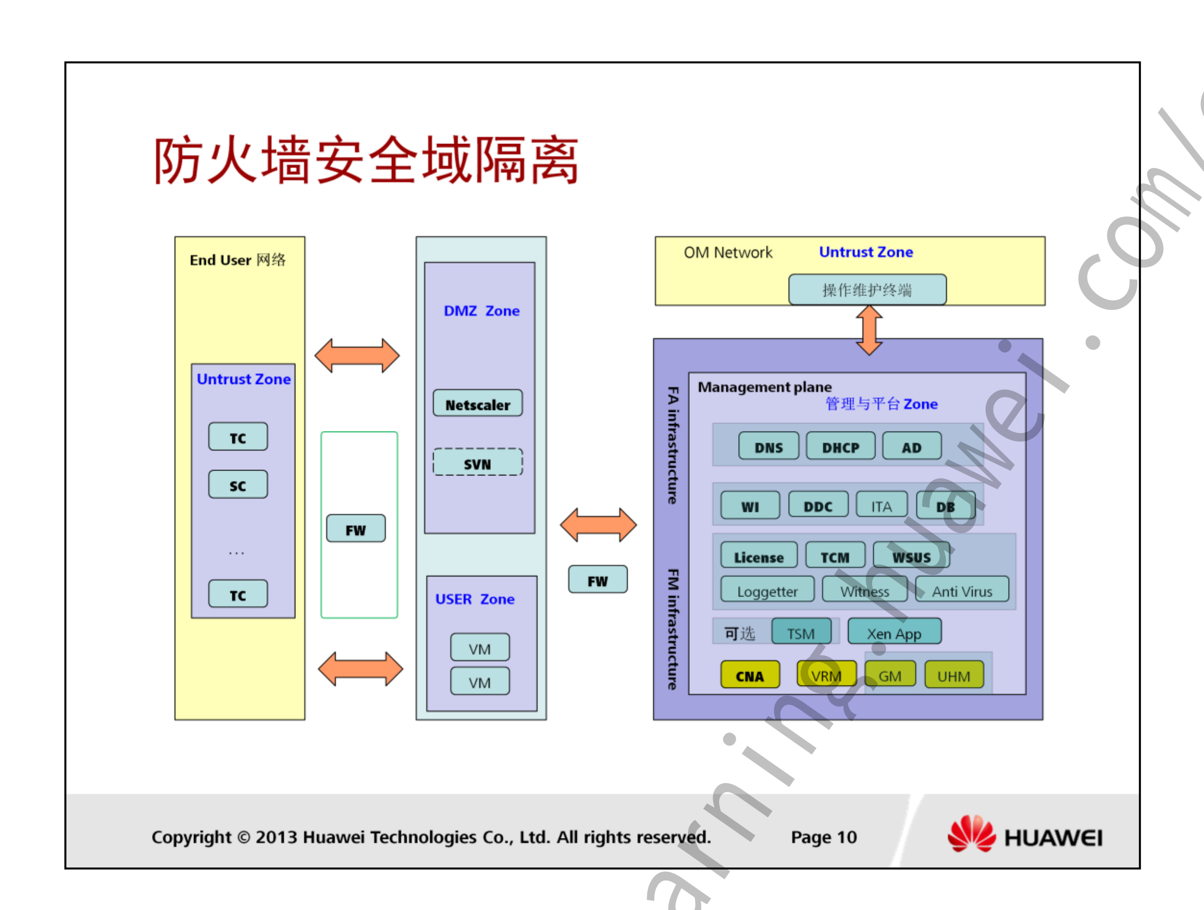


安全接入网关



- 所有网络访问必须经过Netscaler/SVN，确保网络接入安全；
- Netscaler 具有“应用安全和防火墙功能”：能够防御拒绝服务攻击 (DoS)，如SYN Flood 攻击。能保护各项应用免遭黑客和恶意软件滥用，如跨站点脚本攻击、缓冲区溢出攻击、SQL 注入攻击等。
- 访问控制列表：将传入的数据包与访问控制列表 (ACL) 进行比较。如果数据包与 ACL 规则相匹配，则规则中指定的操作将应用于该数据包。





- FA: **FusionAccess**
- **FM: FusionManager**

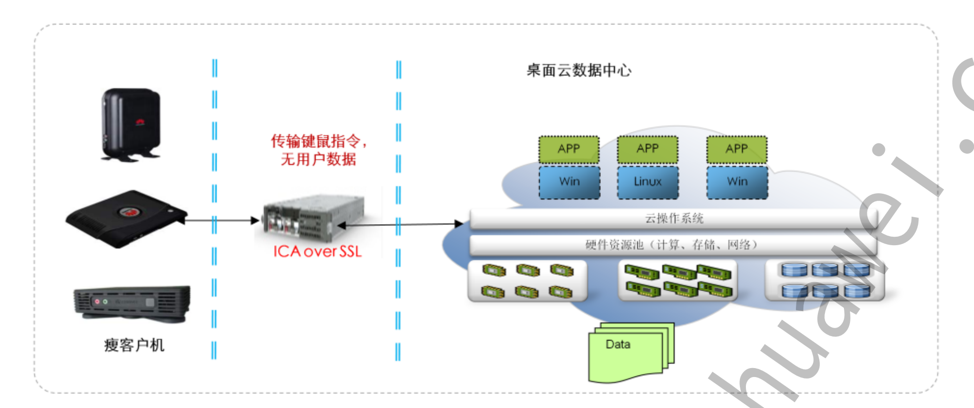


目录

2. 终端及接入安全



终端及外设管控



- 终端与信息分离，桌面和数据在后台集中存储和处理，**传输到终端的仅是屏幕图像和键盘/鼠标指令，无用户数据，且传输是加密的**
- **TC USB外设进行精细化控制**：仅支持键盘鼠标，及指定型号的USB key（用于USB key认证）和指纹仪（用于指纹认证），做到用户无法拷出数据

 Page 12 HUAWEI



防止非法TC接入

- **应对安全威胁场景：**
  - 恶意用户带入无安全措施的TC接入桌面云虚拟机，如在TC上安装录屏软件，通过录屏软件获取机密信息，导致信息泄露
- **解决方案原理：**
  - 在TC出厂时或部署前由管理员用专用工具导入证书（证书只能导入，不能导出），TC接入桌面云的接入网关时进行SSL的双向认证，只有合法TC才能接入
- **部署及配置：**

1、从客户获取给TC颁发的证书及私钥（如果客户无第三方CA，可使用微软的免费CA颁发）

2、使用专用工具（TCM兼有此功能）将证书/私钥及配置脚本打包，导入TC；

3、WI配置SSL双向认证（如是SVN，在接入网关配置）

注：必须在管理上保护好证书和私钥文件，防止外泄



固定TC接入

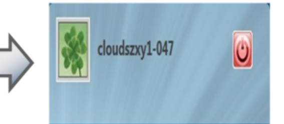
- 应用场景：在信息安全要求高的场合，只允许用户在固定的地点登录包含敏感信息的虚拟桌面，从而避免了敏感信息在其它地方被访问
- 固定TC接入：在TC MAC地址与域和用户名之间建立绑定关系
- 创建TC绑定，如右图所示：



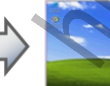
- 登录流程如下图所示：



1.登录WI时，TC会将用户名域名，MAC地址发送桌面云系统，检查TC是否与此用户绑定



2.与预先配置相匹配，则允许去AD鉴权，继续登录过程，否则不允许继续登录



3. AD鉴权通过，成功登录进入VM

 Page 14 HUAWEI





目录

2. 终端及接入安全



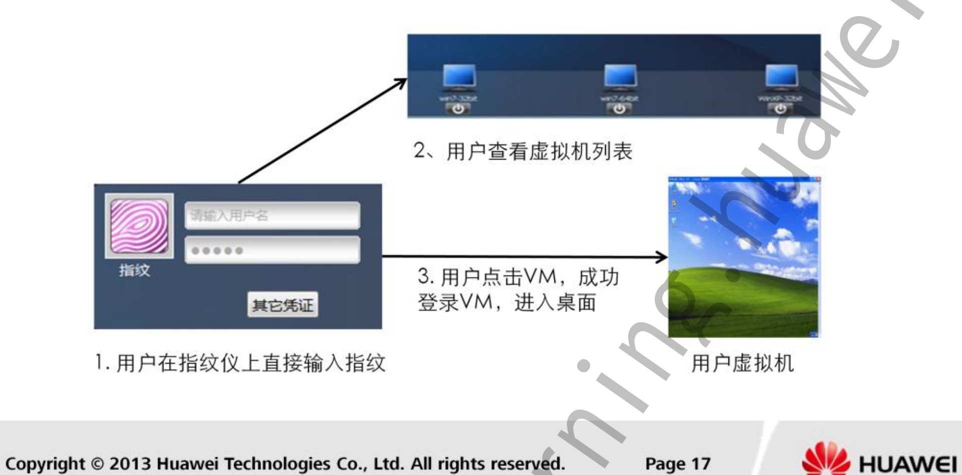
域帐号密码认证

- 用户接入虚拟机必须经过认证，认证方式支持四种：**域帐号+密码、指纹、USB Key、动态口令**，以满足企业不同安全级别的需求
- 域认证：采用微软AD进行用户虚拟机帐号的集中管理，只有认证通过才可接入

- **支持单点登录（SSO）虚拟机**，方便快捷，只要输入一次域帐号密码。流程如下：

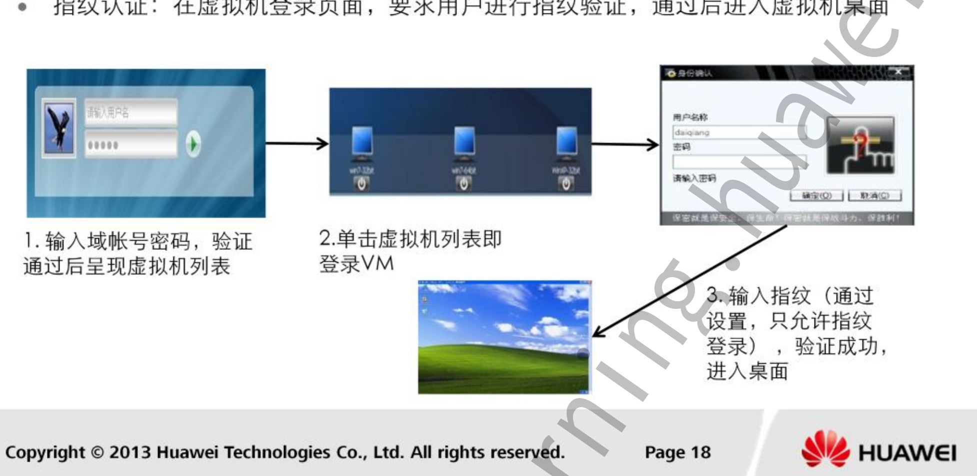
指纹强认证

- 密码安全风险：密码属于一种较弱认证方式，容易通过猜测、截获等方式获取
- 指纹认证：利用指纹生物特征进行强认证，难以伪造和破解，使用起来比较便利
- 单点登录：用户在WI直接输入一次指纹即可登录，无需输入账号密码，方便快捷



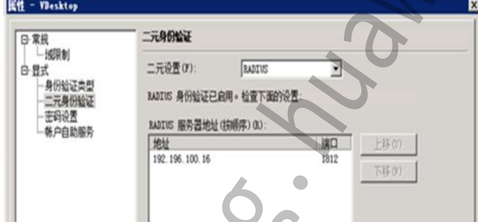
指纹双因素认证

- 域和指纹双因素认证：是将域账号密码与指纹技术相结合，仅当通过域账号密码和指纹的双重认证才允许用户访问桌面云，提高用户桌面的安全性
- 域账号密码：用户在WI输入域账号密码，选择虚拟机登录
- 指纹认证：在虚拟机登录页面，要求用户进行指纹验证，通过后进入虚拟机桌面



动态口令双因素认证

- 动态口令双因素认证：在桌面云WI登录认证时，采用域用户密码+令牌卡的动态口令进行认证
- WI配置如右下角图所示：


HUAWEI

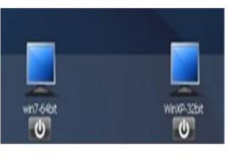
USBKey认证（1）

- USBKey属于智能卡的一种，每个USBKey都具有硬件和PIN码保护，PIN码和硬件构成了两个必要因素（“双因子认证”）
- 场景一：仅需在登录终端时输入一次PIN码，后续即可单点登录WI和VM。
- 应用约束：终端需加入AD域，Linux TC不支持该场景











1.登录终端(XPE TC/SC)，输入一次智能卡PIN码

2.进入终端系统后，在云客户端可直接看到虚拟机列表，无需再次输入PIN码

3.点击某台虚拟机图标，直接登录进入VM,无需再次输入PIN码



USBKey认证（2）

- **场景二：** 登录WI和VM，需要各输入一次PIN码
- **优点：** 支持任何类型的终端（XPE TC/Linux TC/SC），终端无需加入AD域










1.打开云客户端后，浏览器弹出PIN码输入框，用户输入USB Key的PIN码

2.输入正确PIN码后看到虚拟机列表

3.点击虚拟机图标后，在VM登录窗口再次输入USB Key的PIN码

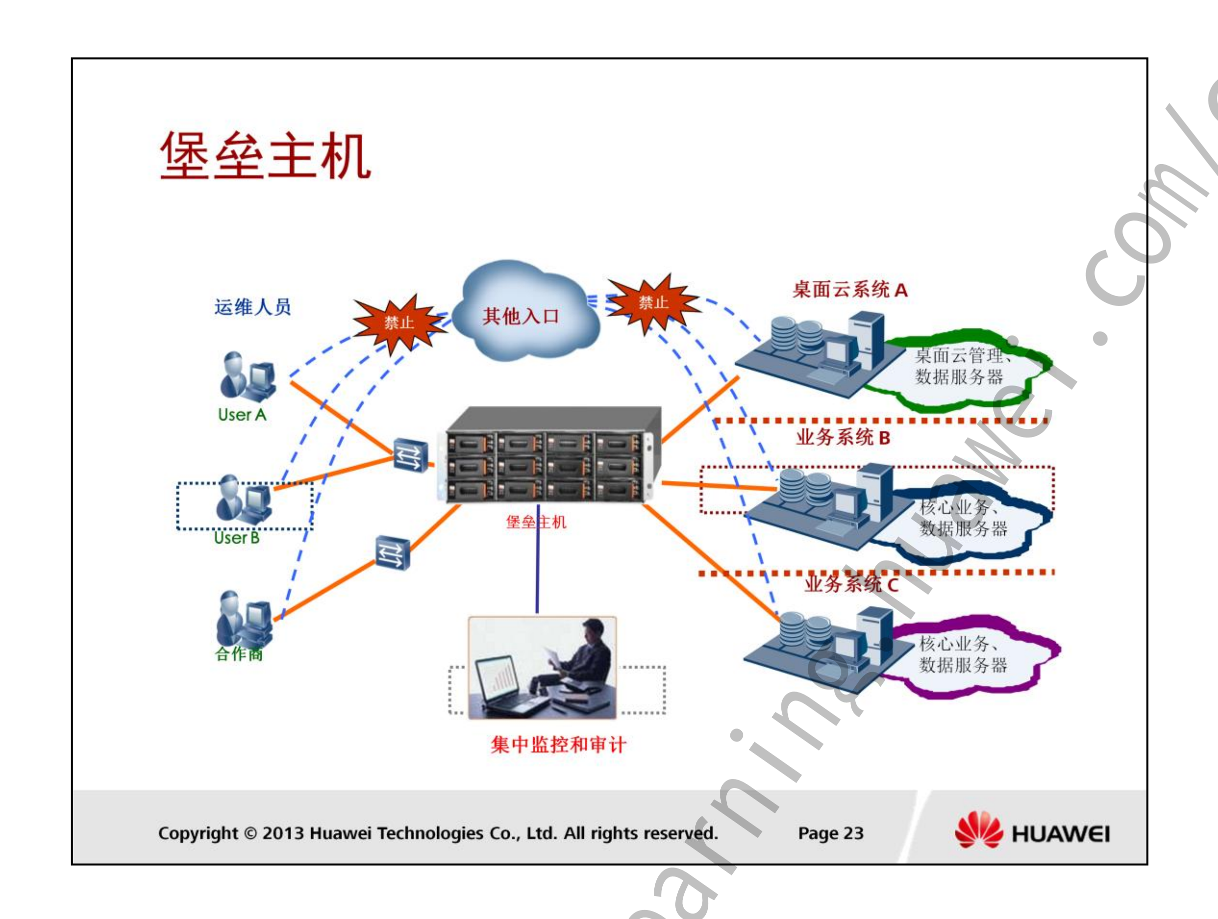
4.输入正确PIN码后，登录进入VM





目录





- **现状：** 多点接入，分散管理，如应用RDP、SSH、SFTP、Https等方式对核心资源进行维护，难以对管理员行为进行审计。
- **解决方案：** 部署堡垒主机，统一运维入口且操作记录日志，支撑审计。



操作名称	操作用户	用户IP	级别	开始时间	结束时间	操作结果	失败原因	详细信息
用户登录	admin	192.102.0.212	一般	2012-03-05 15:57:16	2012-03-05 15:57:16	成功		用户登录：用户名=a
用户登录	admin	192.102.0.212	一般	2012-03-05 15:57:06	2012-03-05 15:57:06	失败	用户名或密码错误	用户登录：用户名=a
用户登录	admin	192.102.0.212	一般	2012-03-05 15:56:53	2012-03-05 15:56:53	失败	用户名或密码错误	用户登录：用户名=a
用户登录	admin	192.102.0.220	一般	2012-03-05 15:27:02	2012-03-05 15:27:02	成功		用户登录：用户名=a
用户登录	admin	192.102.0.220	一般	2012-03-05 15:26:52	2012-03-05 15:26:52	失败	验证码过期	用户登录：用户名=a
用户登录	admin	192.102.0.220	一般	2012-03-05 14:08:20	2012-03-05 14:08:21	成功		用户登录：用户名=a
用户登录	admin	192.102.0.220	一般	2012-03-05 14:07:50	2012-03-05 14:07:50	失败	用户名或密码错误	用户登录：用户名=a

- **管理员操作记录的日志内容详实，能够支撑审计**，包括操作名称、操作用户、用户IP、级别、开始时间、结束时间、操作结果、失败原因、详细信息。
- **日志支持快速搜索，**支持搜索的关键字包括：操作用户、操作时间；
- **日志支持导出，日志定期备份。**

接入操作日志及录像

- 为了应对下面需求，需对用户行为进行监控：
  - 法规要求：
    - 来自外部：例如政府、行业的法律法规；
    - 来自内部：企业的规章制度
  - 保护信息安全：
    - 知识产权的泄漏
    - 敏感数据和客户信息的泄漏
- 如下图示应用虚拟化场景（Xenapp）



HUAWEI

- **应用虚拟化场景（Xenapp）：**

  支持对用户行为进行录像，通过三步完成，右图所示。

  1.配置：管理员配置需监控用户、应用或服务器；

  2.录像：在指定服务器上高效存储屏幕录像，并对每个录像文件数字签名以保证安全；

  3.审计：管理员或审计部门可以搜索已存录像并在内置播放器中审查。

- **虚拟桌面场景（VM）：**

  1.用户接入桌面云，在接入网关有详细的日志记录：如接入IP、接入时间、接入的VM地址；

  2.在企业有特殊需求的情况下，可对用户行为进行进行远程监控（解决方案默认不提供）



2. 终端及接入安全

2.1 用户接入控制

2.2 终端接入控制

2.3 防止非法用户接入

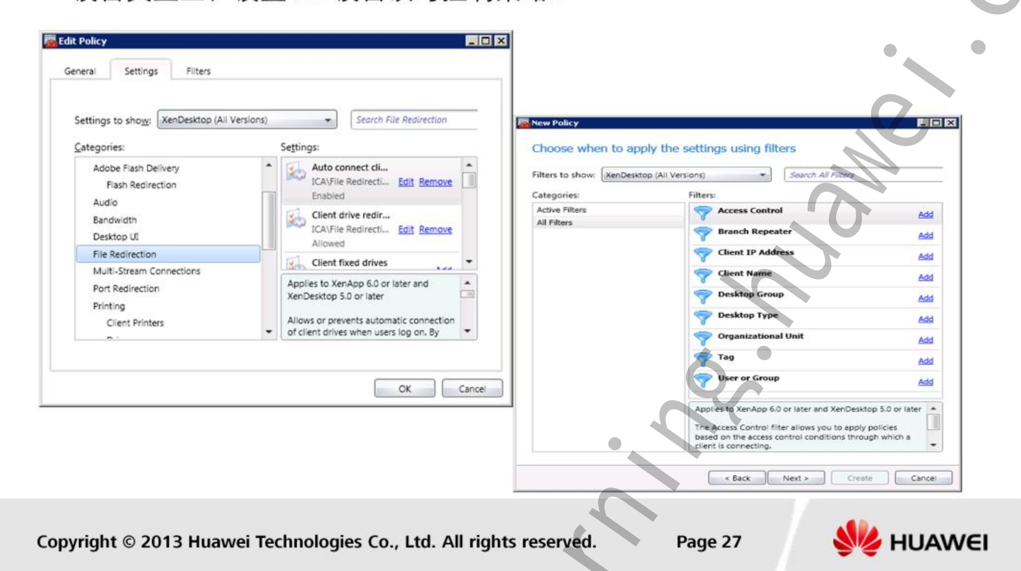
2.4 安全合规审计

2.5 USB端口策略管控



USB端口策略管控（1）

- 通过Citrix Desktop Studio设置，在File Redirection类别的Removable设备类型上，设置USB设备读写控制策略。

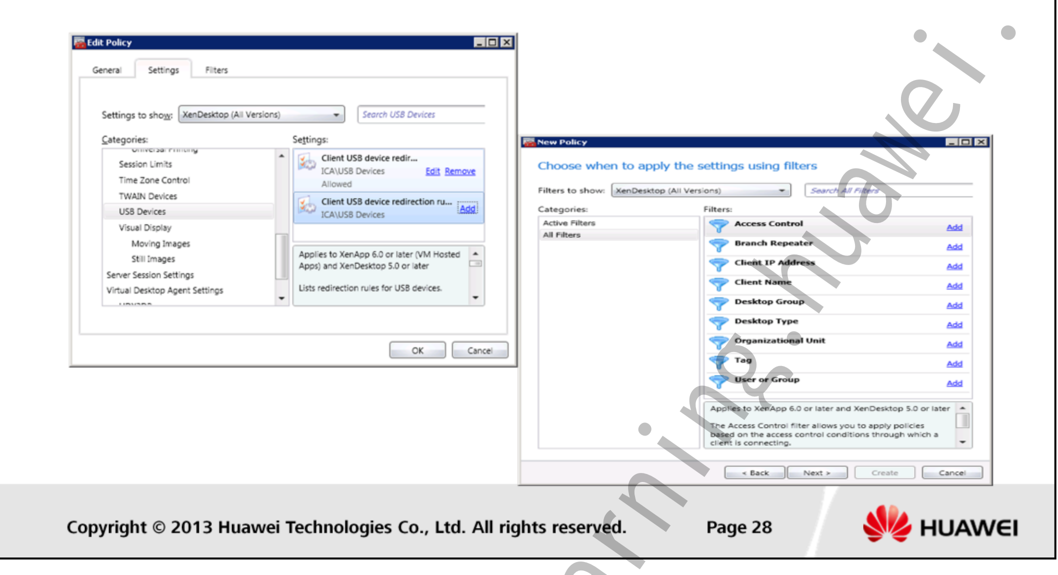


Page 27
HUAWEI

- 通过Citrix Desktop Studio设置，在File Redirection类别的Removable设备类型上，设置USB设备读写控制策略。
  - 可打开或关闭该策略。该策略针对可移动存储设备，包括USB设备、移动硬盘。
  - 可限定该策略应用到的范围，包括指定的终端IP地址、指定的桌面组、指定的桌面组类型、OU、用户或者用户组。

USB端口策略管控（2）

- 通过Citrix Desktop Studio设置，在USB Devices类别上设置USB设备读写控制策略。



- 通过Citrix Desktop Studio设置，在USB Devices类别上设置USB设备读写控制策略。
    - 可打开或者关闭该策略，该策略针对通用USB设备，比如指纹仪等。
    - USB设备策略，可以配置如下设备描述标识进行过滤，包括：VID、PID、REL、Class、Sub-Class、Prot。
    - 可限定该策略应用到的范围，包括：指定的终端IP地址、指定的桌面组、指定的桌面组类型、OU、用户或者用户组。



目录

1. 云安全基本知识
2. 终端及接入安全
3. **网络安全**
4. 虚拟化软件安全
5. 数据安全
6. 运维安全
7. 基础设施安全





3. 网络安全

3.1 防火墙基本原理

3.2 防火墙基本概念及功能



什么叫防火墙?

- 防火墙(Fire Wall)：简单的说，网络安全的第一道防线，是位于两个信任程度不同的网络之间（如企业内部网络和Internet之间）的设备，它对两个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问以达到保护系统安全的目的
- 防火墙 = 硬件 + 软件 + 控制策略
  - 宽松控制策略：除非明确禁止，否则允许
  - 限制控制策略：除非明确允许，否则禁止
- 防火墙的特性：
  - 内部和外部之间的所有网络数据流必须经过防火墙
  - 只有被安全政策允许的数据包才能通过防火墙
  - 防火墙本身要具有很强的抗攻击、渗透能力



 Page 31 HUAWEI

- 在逻辑上，防火墙是分离器，限制器，也是一个分析器，有效地监控了内部网和外部网之间的任何活动，保证了内部网络的安全。
- 在物理上，防火墙通常是一组硬件设备——路由器、主计算机，或者是路由器、计算机和配有软件的网络的组合。
- 防火墙一般可分为多个部分，某些部分除了执行防火墙功能外还执行其它功能。如：加密和解密——VPN。

- 两种极端的表现形式：
  - 限制政策，安全但不好用。（限制政策）
  - 宽松政策，好用但不安全。（宽松政策）
  - 多数防火墙都在两种之间采取折衷。

防火墙的功能

- 防火墙能提供的功能
  - 监控和审计网络的存取和访问：过滤进出网络的数据，管理进出网络的访问行为，封堵某些禁止的业务，记录通过防火墙的信息内容和活动，对网络攻击进行检测和告警
  - 部署于网络边界，兼备提供网络地址翻译(NAT)、虚拟专用网(VPN)等功能
  - 防病毒、入侵检测、认证、加密、远程管理、代理 ……
  - 深度检测对某些协议进行相关控制
  - 攻击防范，扫描检测等



 Page 32



- 防火墙和传统网络设备路由器有一个很大的区别就是：路由器设备只关注网络层的内容，根据IP地址查找出接口完成报文的正确转发，对于应用层的内容路由器是不关心的，完成异构网的互联互通是路由器本质的一个功能。由于IP协议本身的特点，因此非常容易在应用层携带很多有害于网络的内容，造成网络的安全隐患。

防火墙种类和关键技术

- 按照防火墙产品类型分类：软件防火墙、硬件防火墙
- 按照防范方式和相关技术分类：
  - 包过滤防火墙(Packet Filtering)
  - 代理型防火墙(Application Gateway)
  - 状态检测防火墙(Stateful Inspection)
- 防火墙的关键技术
  - 包过滤技术
  - 代理技术
  - 状态检测技术
  - 网络地址翻译 NAT
  - 虚拟专用网 VPN
  - 应用协议特定的包过滤技术ASPF
  - QOS技术
  - 应用层流控技术包括P2P限流
  - 防攻击技术，DPI技术

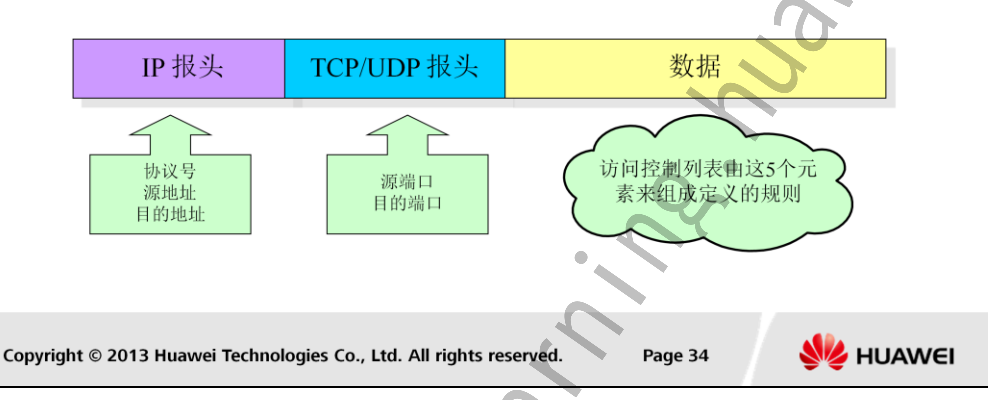


 Page 33 HUAWEI



包过滤防火墙(Packet Filtering)

- 包过滤防火墙(Packet Filtering)
  - 此类防火墙布放在网络中的适当位置，利用数据包的五元组的部分或者全部的信息，按照定义的规则ACL对通过的数据包进行过滤。这是一种基于网络层的安全技术，对于应用层的黑客行为无能为力
  - 包过滤防火墙简单，但是缺乏灵活性；包过滤防火墙每包需要都进行策略检查，策略过多会导致性能急剧下降；
  - 包过滤防火墙对于任何应用需要配置双方向的ACL规则，不能提供差异性保护

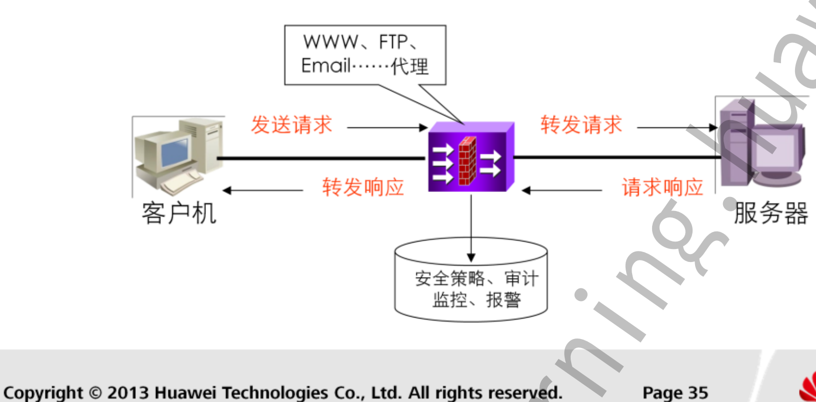


 Page 34 HUAWEI

- 根据流经该设备的数据包地址信息，决定是否允许该数据包通过，判断依据有：
  - 数据包协议类型：TCP、UDP、ICMP、IGMP等
  - 源、目的IP地址
  - 源、目的端口：FTP、HTTP、DNS等
  - IP选项：源路由、记录路由等
  - TCP选项：SYN、ACK、FIN、RST等
  - 其它协议选项：ICMP ECHO、ICMP ECHO REPLY等
  - 数据包流向：in或out
  - 数据包流经网络接口：eth0、eth1
- 包过滤的优点：
  - 不用改动应用程序、一个过滤防火墙能协助保护整个网络、数据包过滤对用户透明、过滤防火墙速度快、效率高。
- 包过滤的缺点：
  - 不能彻底防止地址欺骗；一些应用协议不适合于数据包过滤（如UDP协议）；正常的数据包过滤防火墙无法执行某些安全策略；安全性较差 ；数据包工具存在很多局限性。

代理型防火墙(Application Gateway)

- 代理型防火墙（application gateway）
  - 代理型防火墙使得防火墙做为一个访问的中间节点，对Client来说防火墙是一个Server，对Server来说防火墙是一个Client，转发性能低；
  - 此类防火墙安全性较高，但是开发代价很大。对每一种应用开发都需要一个对应的代理服务，因此代理型防火墙不能支持很丰富的业务，只能针对某些应用提供代理支持
  - 代理型防火墙很难组成双机热备的组网，因为状态无法保持同步



 Page 35



- 代理技术的优点

  1）代理易于配置。

  2）代理能生成各项记录。

  3）代理能灵活、完全地控制进出流量、内容。

  4）代理能过滤数据内容。

  5）代理能为用户提供透明的加密机制。

  6）代理可以方便地与其他安全手段集成。

- 代理技术的缺点

  1）代理速度较路由器慢。

  2）代理对用户不透明。

  3）对于每项服务代理可能要求不同的服务器。

  4）代理服务不能保证免受所有协议弱点的限制。

  5）代理不能改进底层协议的安全性。

状态检测防火墙

- 状态检测防火墙
  - 状态检测是一种高级通信过滤。它检查应用层协议信息并且监控基于连接的应用层协议状态。对于所有连接，每一个连接状态信息都将被ASPF维护并用于动态地决定数据包是否被允许通过防火墙或丢弃。
  - 状态检测技术在网络层实现所有需要的防火墙能力，它既有包过滤机制的速度和灵活，也有代理理型防火墙安全的优点

采用状态检测技术的防火墙产品是现在的主流

 Page 36 

- 状态检测防火墙有如下的优点：

  1. 高安全性
  2. 高效性
  3. 伸缩性和易扩展性
  4. 针对性
  5. 应用范围广

防火墙主要性能衡量指标

1、吞吐量：是指防火墙对报文的处理能力

业界一般都是使用1K～1.5Kbyte的大包来衡量防火墙对报文的处理能力。但网络流量大部分是200Byte字节报文，因此需要考察防火墙小包下转发性能。同时由于防火墙需要配置规则，因此还需要考察防火墙支持ACL下的转发性能。

2、每秒建立连接速度：指的是每秒钟可以通过防火墙建立起来的完整TCP连接

由于防火墙的连接是根据当前通信双方状态而动态建立的。每个会话在数据交换之前，在防火墙上都必须建立连接。如果防火墙建立连接速率较慢，在客户端反映是每次通信有较大延迟。因此支持的指标越大，转发速率越高。在受到攻击时，这个指标越大，抗攻击能力越强。这个指标越大，状态备份能力越强。

3、并发连接数目：是指的可以同时容纳的最大的连接数目

由于防火墙是针对连接进行处理报文的，并发连接数目是指的防火墙可以同时容纳的最大的连接数目，一个连接就是一个TCP/UDP的访问





目录

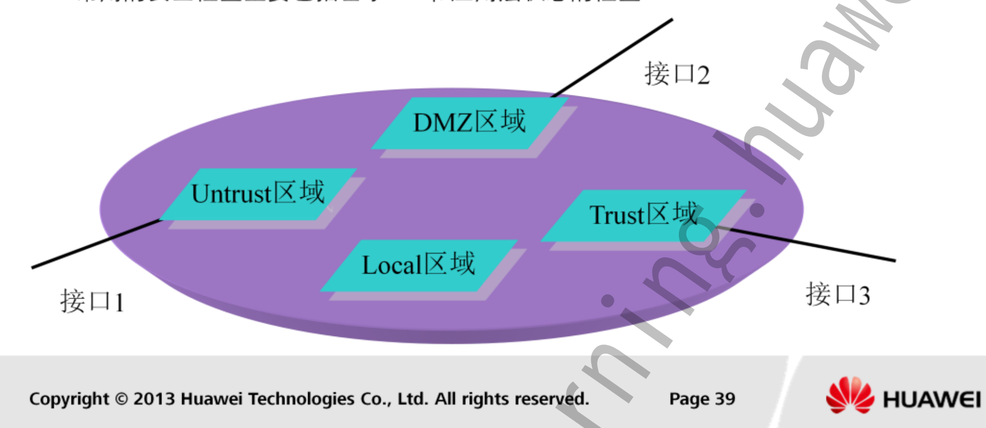


防火墙基本概念 - 安全区域

防火墙的内部划分为多个区域，所有的转发接口都唯一的属于某个区域。

- 域（Zone）

  域是防火墙上引入的一个重要的逻辑概念；通过将接口加入域并在安全区域之间启动安全检查（称为安全策略），从而对流经不同安全区域的信息流进行安全过滤。常用的安全检查主要包括基于ACL和应用层状态的检查



 Page 39 HUAWEI

- Eudemon防火墙上预定以了4个安全区域：本地区域（Local）、受信区域（Trust）、非军事化区域（DMZ）、非受信区域（Untrust），用户根据需要可以自行添加新的安全区域。
- 通常，Eudemon内部处理模块自身所占据的区域就是Local区域，需要保护的内部网络被部署在Trust区域，向外部提供各种服务（如FTP服务器）的网络被部署在DMZ区域，所有外部网络都为Untrust区域。
- 说明：
- 按照优先级从高到低顺序为Local->Trust->DMZ->Untrust，安全级别分别为100、85、50和5，各安全区域具有互不相同的优先级。最多可以为Eudemon配置16个安全区域。

防火墙基本概念 - 域间

- 域间（InterZone）：

  防火墙在引入域概念的同时也引入了域间概念；任何不同的安全域之间形成域间关系，Eudemon防火墙上大部分规则都是配置在域间上，为了便于描述同时引入了域间方向的概念

- inbound：

  报文从低优先级区域进入高优先级区域为入方向

- outbound：

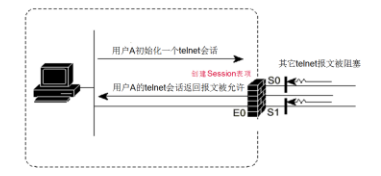
  报文从高优先级区域进入低优先级区域为出方向



防火墙基本概念 - 会话

- 会话

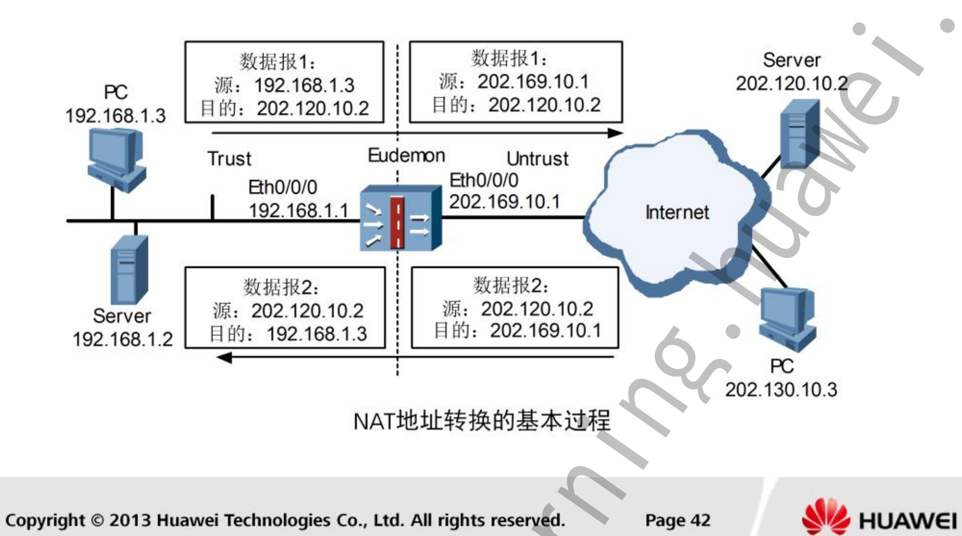
  会话是状态防火墙的基础，每一个通过防火墙的会话都会在防火墙上建立一个会话表项，以五元组（源目的IP地址、源目的端口、协议号）为Key值；通过建立动态的会话表来可以提供高优先级域更高的安全性，即如下图所示高优先级域可以主动访问流的等价路由，应用层流控等





防火墙基本概念 - NAT

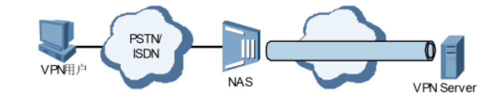
- NAT（Network Address Translation，地址转换）是将IP数据报报头中的IP地址转换为另一个IP地址的过程



NAT地址转换的基本过程

防火墙基本概念 - VPN

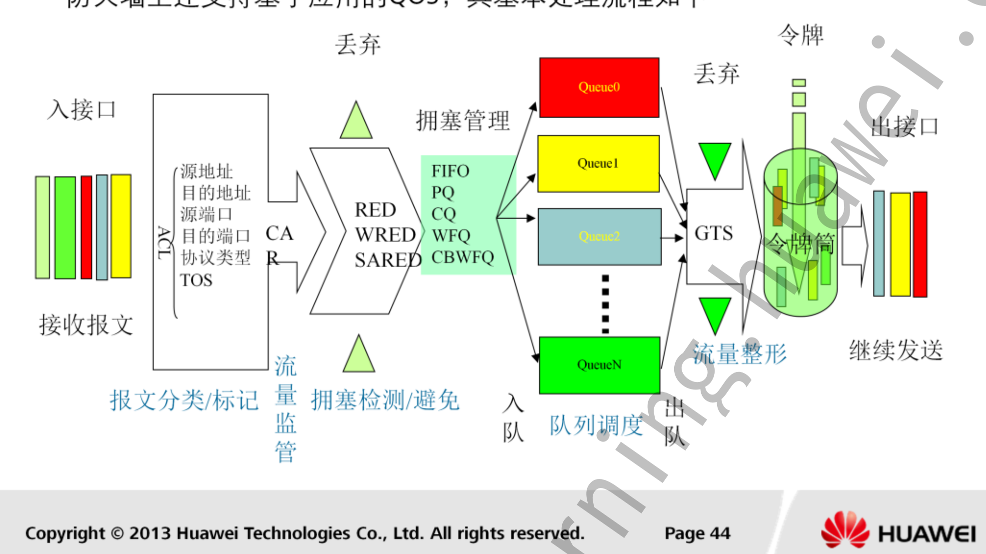
- 虚拟私有网（Virtual Private Network）简称VPN，是近年来随着Internet的广泛应用而迅速发展起来的一种新技术，用以实现在公用网络上构建私人专用网络。“虚拟”主要指这种网络是一种逻辑上的网络。目前防火墙上提供L2TP和IPSec VPN服务，
- VPN原理如下图所示，其实质是通过隧道技术让用户通过公网直接访问用户自己的私网：





防火墙基本概念 - 服务质量保证

- QOS：服务质量保证，是数通设备需要提供的基于服务的品质保证服务，防火墙上还支持基于应用的QOS，其基本处理流程如下



防火墙基本概念 - 应用层流控

支持 应用层流控（主要是P2P）特性：

•P2P应用兴起对宽带业务的挑战

首先，P2P应用兴起后颠覆了传统的Internet流量模型，导致用户消耗带宽急剧上升，但是运营商的收入并没有增加；其次，P2P业务在传统的交换机以及路由器上很难识别这是因为P2P业务的端口号不固定，如果做深度检测的话P2P应用大部分报文都是检测不出来的

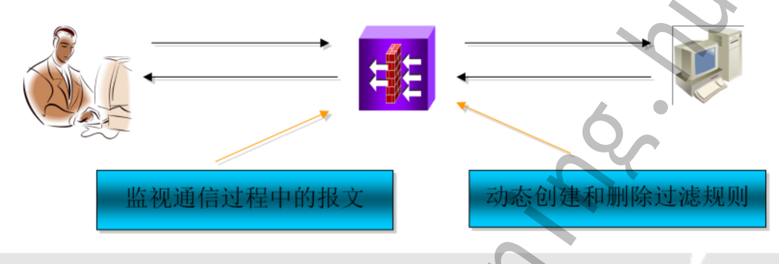
•防火墙在进行P2P限流和应用层限流的优势

防火墙上存在会话表，因此如果会话的应用类型被识别出来之后就很容易对后续报文进行流控，这将极大提高P2P以及应用层流控的效率和准确性



防火墙基本概念 - ASPF

- ASPF(Application Specific Packet Filter)：
  - 是一种改进的高级通信过滤技术，ASPF不但对报文的网络层的信息进行检测，还能对丰富的应用层协议进行深度检测，支持多媒体业务的NAT以及安全防范功能，比如：H323协议族、MGCP、SIP、H248、RTSP、HWCC及ICMP、FTP、DNS、PPTP、NBT、ILS、HTTP、SMTP等
  - 支持对SMTP中的有害命令进行过滤
  - 支持对HTTP中的 Activex/JAVA Appelt 进行过滤





HUAWEI

防火墙基本概念 - 黑名单

- 黑名单，指根据报文的源IP地址进行过滤的一种方式。同基于ACL的包过滤功能相比，由于黑名单进行匹配的域非常简单，可以以很高的速度实现报文的过滤，从而有效地将特定IP地址发送来的报文屏蔽。黑名单最主要的一个特色是可以由Eudemon防火墙动态地进行添加或删除，当防火墙中根据报文的行为特征察觉到特定IP地址的攻击企图之后，通过主动修改黑名单列表从而将该IP地址发送的报文过滤掉。因此，黑名单是防火墙一个重要的安全特性



防火墙基本概念 - Mac地址绑定

- MAC和IP地址绑定，指防火墙可以根据用户的配置，在特定的IP地址和MAC地址之间形成关联关系。对于声称从这个IP发送的报文，如果其MAC地址不是指定关系对中的地址，防火墙将予以丢弃。发送给这个IP地址的报文，在通过防火墙时将被强制发送给绑定的MAC地址，从而形成有效的保护，是避免IP地址假冒攻击的一种方式
- MAC和IP地址绑定功能一般应用在与二层交换机相连的时候，可以防止假冒IP地址攻击，ARP Flood攻击等，还可以应用于用户认证



防火墙基本概念 - 访问控制列表

- ACL（Access Control List，访问控制列表）是防火墙实现数据流控制的手段之一，是防火墙安全策略最基本的规则。ACL根据数据包的源地址、目的地址、端口号、上层协议或其他信息定义一组数据流，并决定是否对该数据流进行后续操作
- Eudemon 中，ACL规则分为基本ACL规则、高级ACL规则和基于MAC地址的ACL规则 和基于防火墙的ACL
- ACL规则因为其能实现复杂的流分类特性而被广泛应用在防火墙各模块，几乎需要进行流分类的模块都使用ACL进行流分类



防火墙基本概念 - 统计

- 统计功能：防火墙上面有很多统计功能，其中除了常用统计外还有会话数的统计，应用服务流量的统计，单个IP地址的统计等，这些统计为防火墙提供了额外功能：
  - 会话数限制
  - 应用层流控
  - 应用统计
  - IP Car



Page 50



防火墙基本概念 - 端口映射

- 端口映射：是解决端口和服务类型映射关系的一个配置功能，对于使用非知名端口提供知名服务时的业务识别非常有用，典型的ftp的服务端口是21，如果有些用户将1021端口作为ftp的服务端口，可以通过PortMap命令来绑定该对应关系，这样1021端口的服务就被自动识别成ftp服务了，另外如果该端口只对特定地址有效可以通过ACL来限制识别范围





防火墙基本概念 - 日志（log）

- 防火墙作为安全设备，除了提供通常的日志外还提供很多与安全相关的日志信息，包括用户每次会话的详细信息，攻击日志，应用流量日志等
- 二进制日志：记录了用户每个会话的详细信息，可供后续分析统计使用
- 应用流量日志：记录了防火墙上识别出来的各种应用的流量数据
- 攻击日志：记录了防火墙上收到的各种攻击的信息
- 黑名单日志：记录用户被加入删除的详细情况





目录





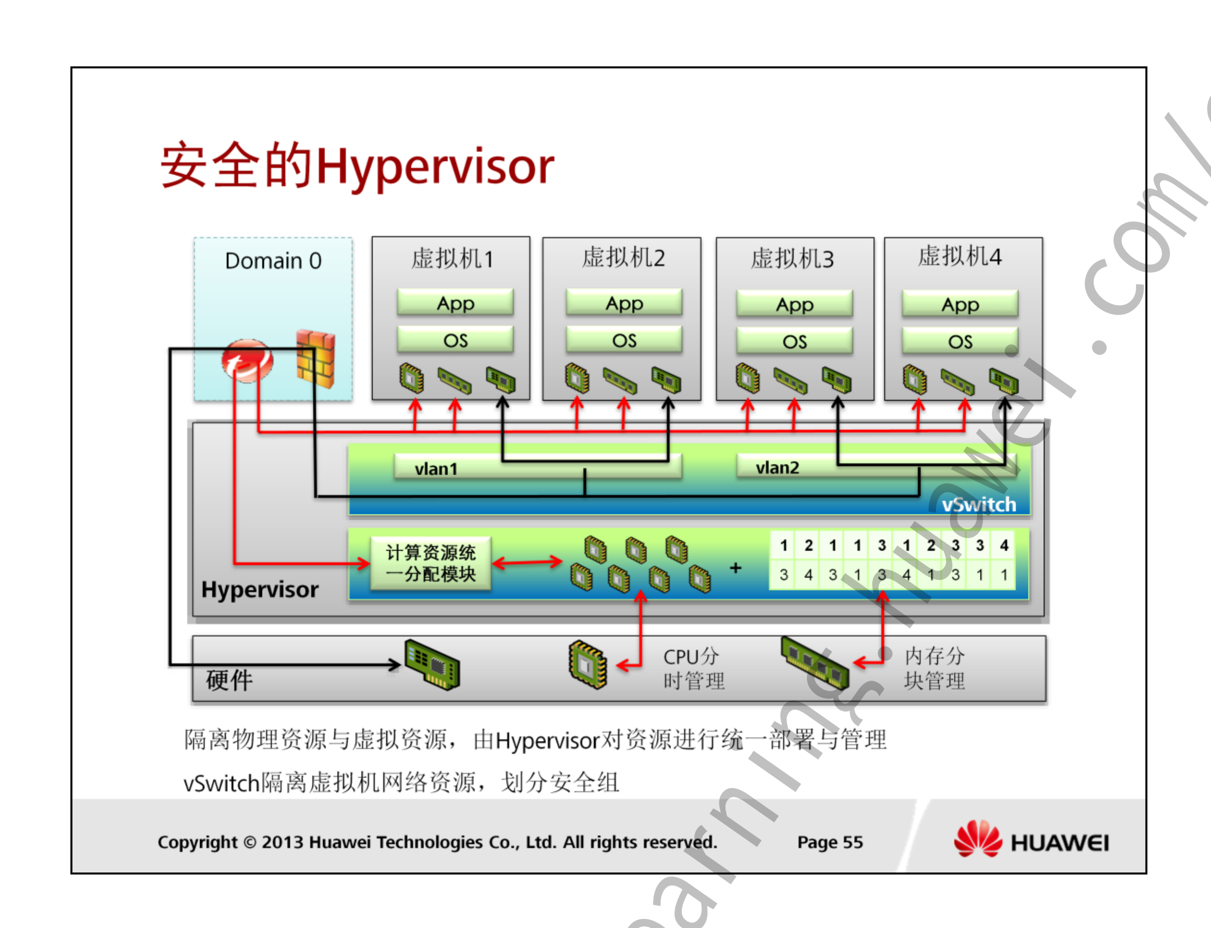
目录

4. **虚拟化软件安全**

    4.1 Hypervisor安全

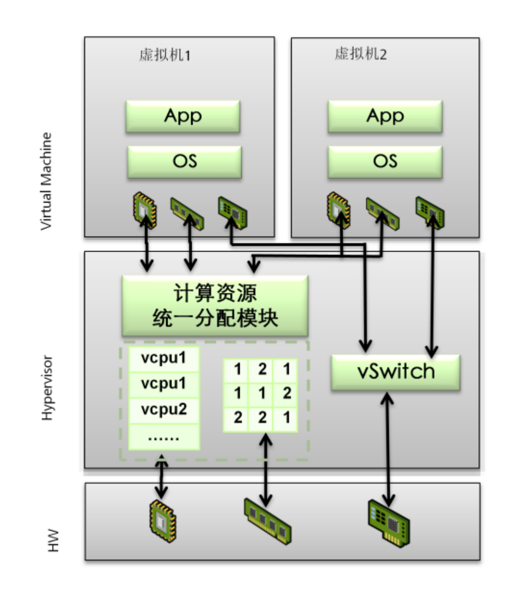
    4.2 虚拟化管理安全





Hypervisor能实现同一物理机上不同虚拟机之间的资源隔离，避免虚拟机之间的数据窃取或恶意攻击，保证虚拟机的资源使用不受周边虚拟机的影响。终端用户使用虚拟机时，仅能访问属于自己的虚拟机的资源（如硬件、软件和数据），不能访问其他虚拟机的资源，保证虚拟机隔离安全。

虚拟机安全隔离



物理资源与虚拟资源的隔离

- Hypervisor统一管理物理硬件资源，保证每个虚拟机都能获得相对独立的资源；
- 屏蔽虚拟资源故障，虚拟机崩溃不影响Hypervisor及其他虚拟机

虚拟机之间的隔离

- Hypervisor从物理层面隔离虚拟机各类资源，使得虚拟机在整个生命周期内互不可见，避免虚拟机之间的数据窃取或恶意攻击；
- 支持定制每个虚拟机的资源配额，保证虚拟机的资源使用不受周边虚拟机的影响

 Page 56 

- **vCPU调度隔离安全**
- X86架构为了保护指令的运行，提供了指令的4个不同Privilege特权级别，术语称为Ring，优先级从高到低依次为Ring 0（被用于运行操作系统内核）、Ring 1（用于操作系统服务）、Ring 2（用于操作系统服务）、Ring 3（用于应用程序），各个级别对可以运行的指令进行限制。vCPU的上下文切换，由Hypervisor负责调度。Hypervisor使虚拟机操作系统运行在Ring 1上，有效地防止了虚拟机Guest OS直接执行所有特权指令；应用程序运行在Ring 3上，保证了操作系统与应用程序之间的隔离。
- **内存隔离**
- 虚拟机通过内存虚拟化来实现不同虚拟机之间的内存隔离。内存虚拟化技术在客户机已有地址映射（虚拟地址和机器地址）的基础上，引入一层新的地址——“物理地址”。在虚拟化场景下，客户机OS将“虚拟地址”映射为“物理地址”；Hypervisor负责将客户机的“物理地址”映射成“机器地址”，实际物理地址后，再交由物理处理器来执行。
- **内部网络隔离**
- Hypervisor提供虚拟防火墙——路由器（VFR，Virtual Firewall - Router）的抽象，每个客户虚拟机都有一个或者多个在逻辑上附属于VFR的网络接口VIF（Virtual Interface）。从一个虚拟机上发出的数据包，先到达Domain 0，由Domain 0来实现数据过滤和完整性检查，并插入和删除规则；经过认证后携带许可证，由Domain 0转发给目的虚拟机；目的虚拟机检查许可证，以决定是否接收数据包。

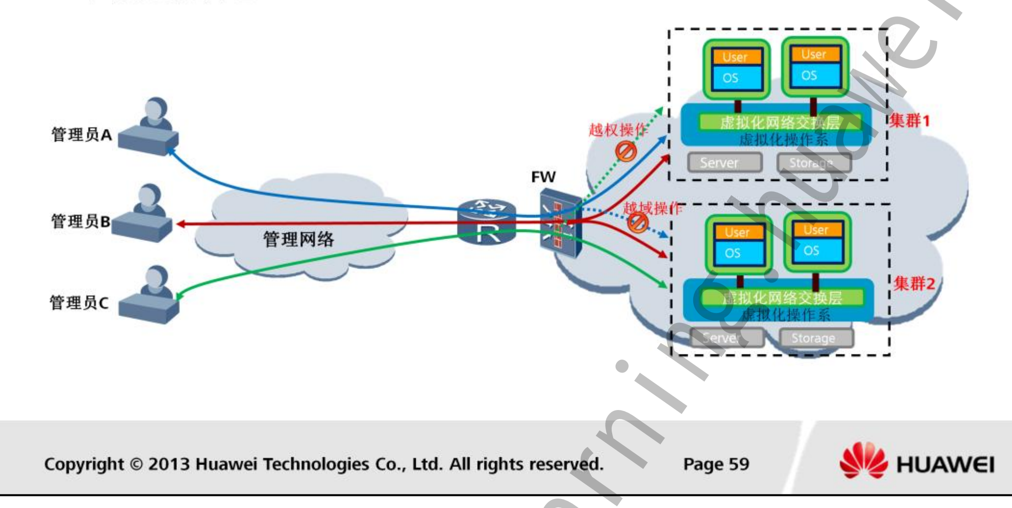


目录



分权分域管理

- 管理员对设备和业务的管理，支持“分权分域管理模式”，遵循NIST标准的RBAC模型，支持灵活的创建角色和管理员，使得管理员不能越权管理



- NIST（The National Institute of Standards and Technology）国家标准技术研究所，是美国商务部的一个部门
- RBAC模型指Role Based Access Control
- **“分权”**：区分操作权限，由“角色”进行控制。一个“角色”可拥有一个或多个不同的“操作权限”，一个“用户”可拥有一个或多个不同的“角色”。通过绑定“用户”和“角色”，实现“用户”和“操作权限”的绑定。
- **“分域”**：区分管理的数据权限，也即管理员能够管理的范围，如“管理员A”仅能管理“集群1”中虚拟机，“管理员C”仅能管理“集群2”中虚拟机。

账号口令安全

- 账号口令满足复杂度要求,认证模块支持防暴力破解
- 账号口令加密存储
  - 对需要还原成明文的口令，采用AES128算法
  - 对不需要还原成明文的口令，采用SHA256
- 云平台机机账号和人机账号分离，支持口令回收
  - 机机账号回收
    - 一个应用对应一个机机账号，由应用提供UI界面修改本端及服务端口令
  - 人机账号回收
    - 用户手工回收或与第三方账号密码管理系统对接

 Page 60 

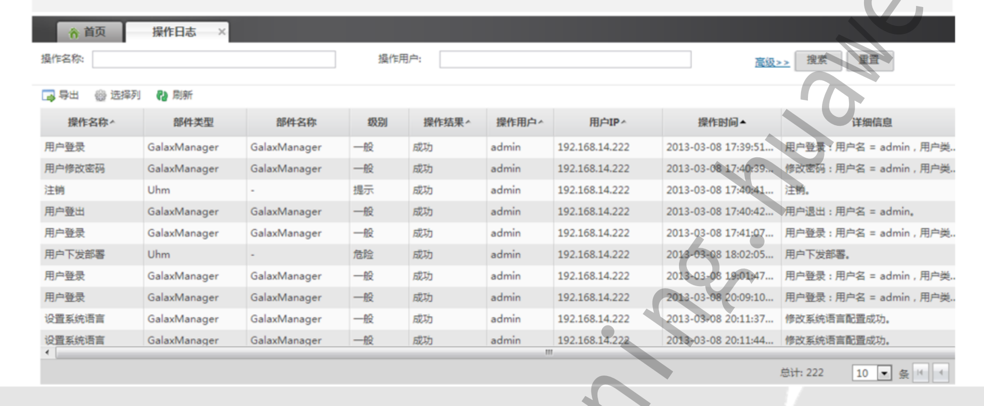
- 口令满足复杂度要求可配置（大小写，字母，特殊字符）,认证模块支持防暴力破解（可配置密码错误多少次之后锁定账号多长时间，系统管理员支持手工解锁）

- 说明1：系统人机账号指：系统安装或配置时缺省设置的管理用账号，以及系统日常维护使用的账号。系统机机账号指：软件、程序、脚本或服务正常运行时需要使用的账号。
- 人机账号是自然人使用的账号，仅能用于系统维护，不能同时作为“机机账号”使用。机机账号是机器使用的账号，仅能用于程序运行，不能同时作为“人机账号”使用。

- 口令支持回收是指云平台用户可以自主修改所有账号口令。在大型公司，一般有自己口令管理规范，比如每3个月要求更换一次系统口令。这种操作一般称为口令回收。

完整的操作日志记录

- **管理员操作记录的日志内容详实，能够支撑审计**，包括操作名称、操作用户、用户IP、级别、开始时间、结束时间、操作结果、失败原因、详细信息等。
- **日志支持快速搜索**，支持搜索的关键字包括：操作用户、操作时间；
- **日志支持导出，日志定期备份。**



操作名称	部件类型	部件名称	级别	操作结果	操作用户	用户IP	操作时间	详细信息
用户登录	GalaxManager	GalaxManager	一般	成功	admin	192.168.14.222	2013-03-08 17:39:51...	用户登录：用户名 = admin，用户类..
用户修改密码	GalaxManager	GalaxManager	一般	成功	admin	192.168.14.222	2013-03-08 17:40:39...	修改密码：用户名 = admin，用户类..
注销	Uhm	-	提示	成功	admin	192.168.14.222	2013-03-08 17:40:41...	注销。
用户登出	GalaxManager	GalaxManager	一般	成功	admin	192.168.14.222	2013-03-08 17:40:42...	用户退出：用户名 = admin。
用户登录	GalaxManager	GalaxManager	一般	成功	admin	192.168.14.222	2013-03-08 17:41:07...	用户登录：用户名 = admin，用户类..
用户下发部署	Uhm	-	危险	成功	admin	192.168.14.222	2013-03-08 18:02:05...	用户下发部署。
用户登录	GalaxManager	GalaxManager	一般	成功	admin	192.168.14.222	2013-03-08 19:01:47...	用户登录：用户名 = admin，用户类..
用户登录	GalaxManager	GalaxManager	一般	成功	admin	192.168.14.222	2013-03-08 20:09:10...	用户登录：用户名 = admin，用户类..
设置系统语言	GalaxManager	GalaxManager	一般	成功	admin	192.168.14.222	2013-03-08 20:11:37...	修改系统语言配置成功。
设置系统语言	GalaxManager	GalaxManager	一般	成功	admin	192.168.14.222	2013-03-08 20:11:44...	修改系统语言配置成功。



目录





目录

5. 数据安全

   5.1 用户数据保护

   5.2 管理数据保护



用户数据访问控制

- 虚拟机所有的I/O操作都会由Hypervisor截获处理，Hypervisor保证虚拟机只能访问分配给该虚拟机的物理磁盘，实现不同虚拟机之间的用户数据隔离。
- 对虚拟机磁盘卸载和挂载操作能独立授权，且有详细的日志记录用于审计。

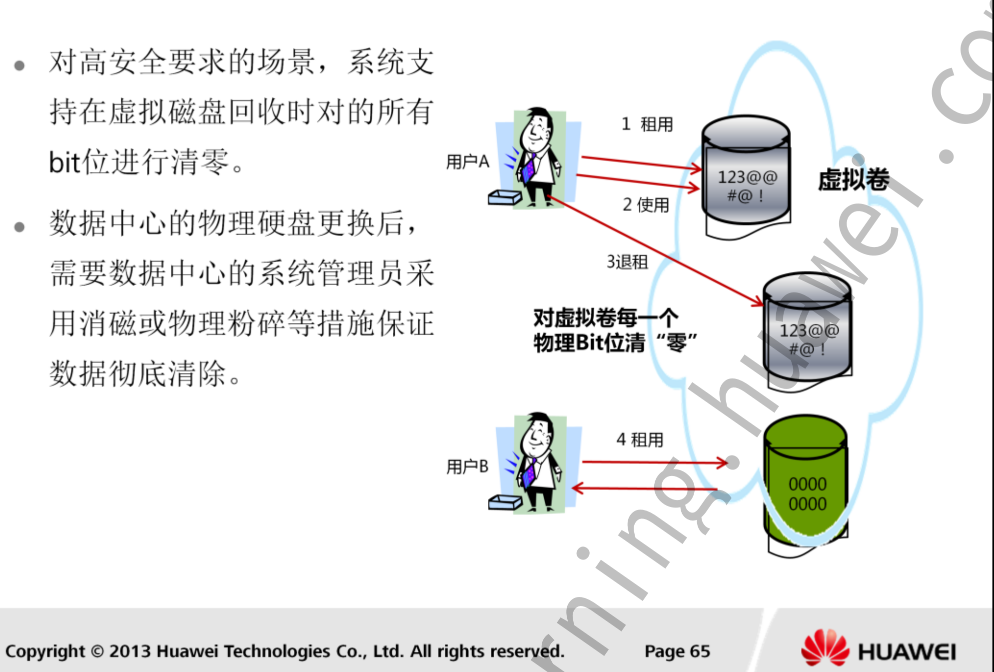
 Page 64



确保VM不会非法访问到其他虚拟机的磁盘:

华为Hypervisor（UVP）采用分离设备驱动模型实现I/O的虚拟化。该模型将设备驱动划分为前端驱动程序、后端驱动程序和原生驱动三个部分，其中前端驱动在DomainU中运行，而后端驱动和原生驱动则在Domain0中运行。前端驱动负责将DomainU的I/O请求传递到Domain0中的后端驱动，后端驱动解析I/O请求并映射到物理设备，提交给相应的设备驱动程序控制硬件完成I/O操作。换言之，虚拟机所有的I/O操作都会由VMM截获处理；VMM保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。

只有高级管理员才能进行虚拟机磁盘卸载和挂载操作，防止非法卸载用户磁盘进行访问。


用户剩余数据安全
对高安全要求的场景，系统支持在虚拟磁盘回收时对的所有bit位进行清零。
数据中心的物理硬盘更换后，需要数据中心的系统管理员采用消磁或物理粉碎等措施保证数据彻底清除。
用户A
1 租用
2 使用
123@@
#@ !
虚拟卷
3退租
对虚拟卷每一个
物理Bit位清“零”
123@@
#@ !
用户B
4 租用
0000
0000
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 65
HUAWEI



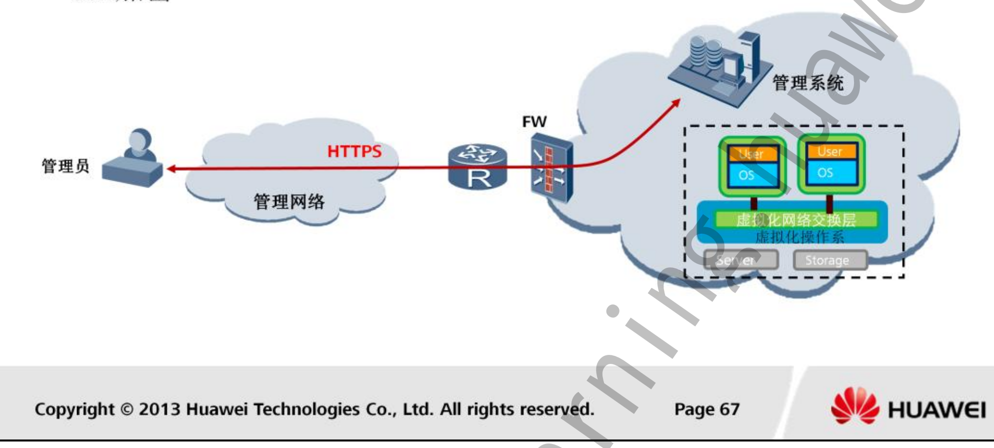
目录

5. 数据安全

   5.1 用户数据保护

   5.2 管理数据保护





- （HTTPS指Hypertext Transfer Protocol Secure ，超文本传输安全协议）（SSL指Secure Sockets Layer ，安全套接层），
- HTTPS可进行加密传输、身份认证，安全性高。HTTPS的安全基础是SSL，通过SSL实现加密，SSL协议提供的服务主要有：
  - 认证用户和服务器，确保数据发送到正确的客户机和服务器。
  - 加密数据以防止数据中途被窃取。
  - 维护数据的完整性，确保数据在传输过程中不被改变。

管理数据加密存储

- 华为云平台对于关键管理数据（例如用户口令，用户个人信息）进行加密保护
- 对于不需要还原数据的场景，使用SHA-256不可逆算法加密
- 对于需要还原数据的场景，使用AES128算法加密



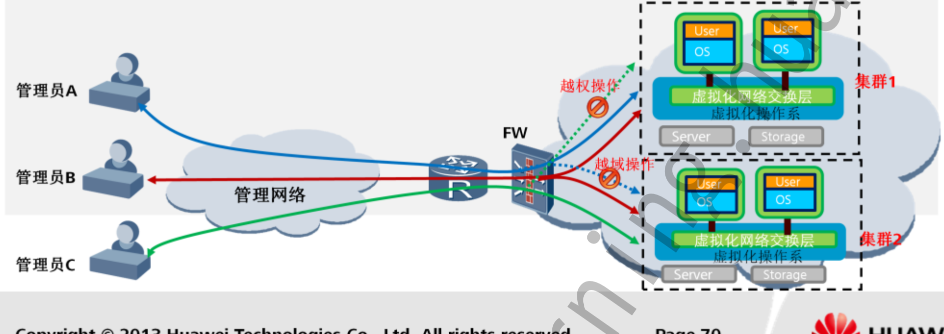


目录



运维安全_分权分域管理

- 管理员对设备和业务的管理，支持“分权分域管理模式”，遵循NIST标准的RBAC模型，基于角色的访问控制
- “分权”：区分操作权限，由“角色”进行控制。一个“角色”可拥有一个或多个不同的“操作权限”，一个“用户”可拥有一个或多个不同的“角色”。通过绑定“用户”和“角色”，实现“用户”和“操作权限”的绑定
- “分域”：区分管理的数据权限，也即管理员能够管理的范围，如“管理员A”仅能管理“集群1”中虚拟机，“管理员C”仅能管理“集群2”中虚拟机。



 Page 70



- NIST（The National Institute of Standards and Technology）
- 其中 NIST指 National Institute of Standards and Technology，国家标准技术研究所，是美国商务部的一个部门，RBAC模型指Role Based Access Control
- 支持灵活的创建角色和管理员，使得管理员不能越权管理。

运维安全_完整操作日志记录

- 管理员操作记录的日志内容详实，能够支撑审计，包括操作名称、操作用户、用户IP、级别、开始时间、结束时间、操作结果、失败原因、详细信息等。
- 日志支持快速搜索，支持搜索的关键字包括：操作用户、操作时间；
- 日志支持导出，日志定期备份。



操作日志

日志搜索

操作用户: -关键字- 操作时段: – <<高级 搜索 重置

操作名称	操作用户	用户IP	级别	开始时间	结束时间	操作结果	失败原因	详细信息
用户登录	admin	192.102.0.212	一般	2012-03-05 15:57:16	2012-03-05 15:57:16	成功		用户登录：用户名=a
用户登录	admin	192.102.0.212	一般	2012-03-05 15:57:06	2012-03-05 15:57:06	失败	用户名或密码错误	用户登录：用户名=a
用户登录	admin	192.102.0.212	一般	2012-03-05 15:56:53	2012-03-05 15:56:53	失败	用户名或密码错误	用户登录：用户名=a
用户登录	admin	192.102.0.220	一般	2012-03-05 15:27:02	2012-03-05 15:27:02	成功		用户登录：用户名=a
用户登录	admin	192.102.0.220	一般	2012-03-05 15:26:52	2012-03-05 15:26:52	失败	验证码过期	用户登录：用户名=a
用户登录	admin	192.102.0.220	一般	2012-03-05 14:08:20	2012-03-05 14:08:21	成功		用户登录：用户名=a
用户登录	admin	192.102.0.220	一般	2012-03-05 14:07:50	2012-03-05 14:07:50	失败	用户名或密码错误	用户登录：用户名=a

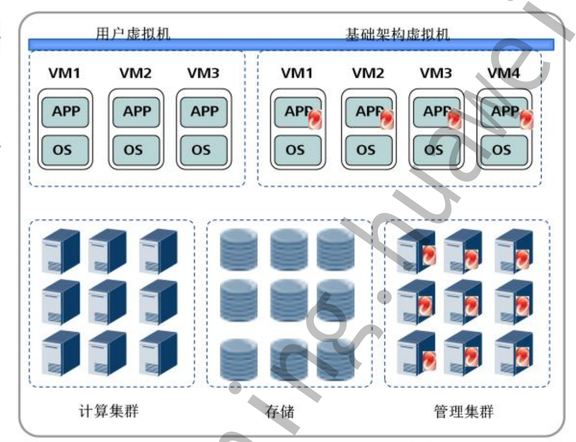


目录



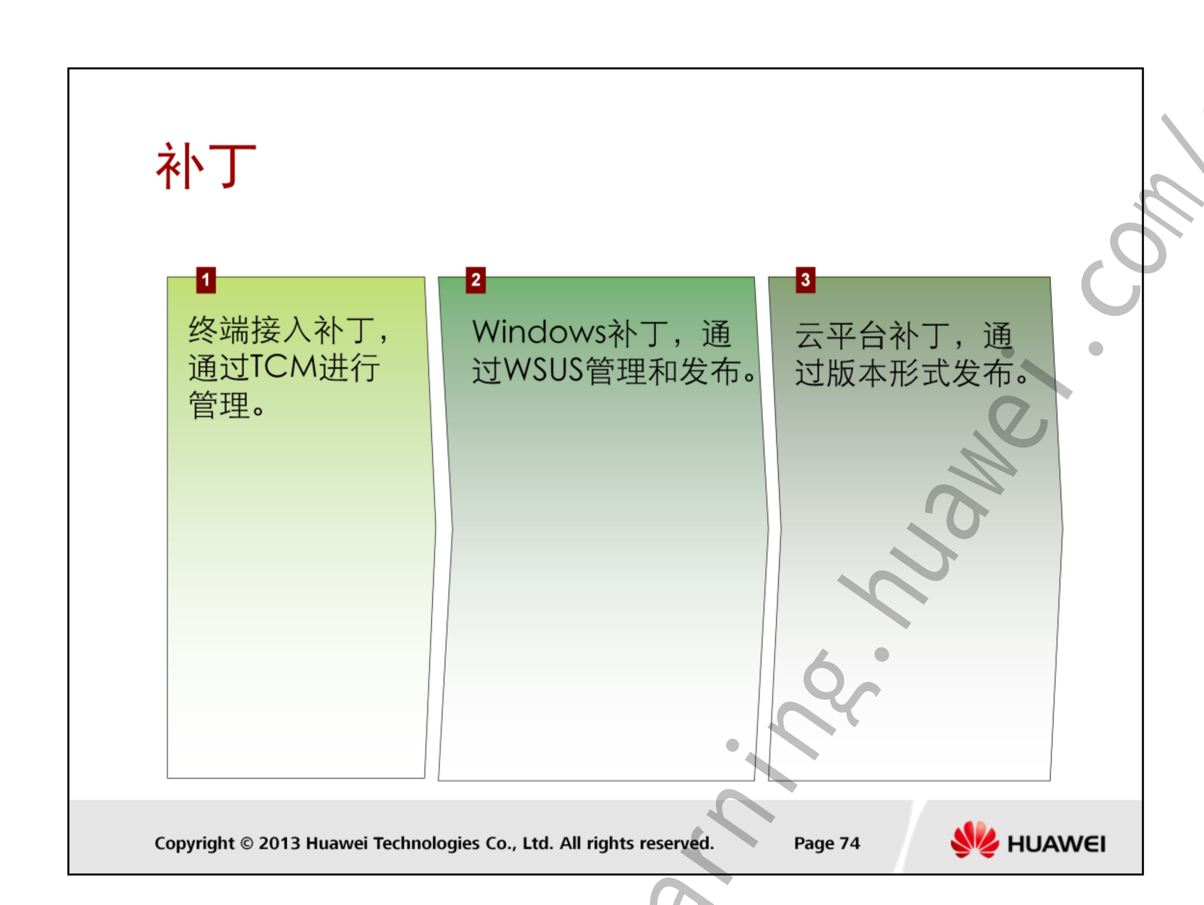
防病毒

- 基础架构虚拟机：必须统一为基础架构虚拟机部署防病毒软件。
- 管理节点：管理节点采用加固的Linux操作系统。
- 计算和存储节点：无需安装防病毒软件。
- 用户虚拟机：支持统一部署防病毒服务器。



Page 73


- 基础架构虚拟机：支持在Windows Server虚拟机上部署趋势的防病毒服务器，为基础架构虚拟机提供防病毒软件功能，通过设置定期任务，定期查杀病毒，防止基础架构虚拟机遭受病毒入侵。
- 管理节点：管理节点采用加固的Linux操作系统。但管理节点提供外部操作平台与外界存在交互操作，因此存在病毒感染风险，但病毒感染风险低
- 计算和存储节点，无需安装防病毒软件，原因如下：
  - 计算和存储节点采用安全加固的Linux操作系统。
  - 计算和存储节点处于封闭网络，且没有提供外部操作平台。
- 用户虚拟机：
  - 支持统一部署防病毒服务器，为用户虚拟机提供防病毒软件功能，通过设置定期任务，定期查杀病毒，防止用户虚拟机遭受病毒入侵。


补丁
1
终端接入补丁，通过TCM进行管理。
2
Windows补丁，通过WSUS管理和发布。
3
云平台补丁，通过版本形式发布。
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 74
HUAWEI



端口矩阵

源设备	源I	源端	目的设备	目的	目的端口	协议	端口说明	目的端口是	认证方	加密方	所属平面	版本	特殊场	备注
DDC/XenApp/ITA/AD/SQL Server/License Server/UserVM	业务平面IP	随机	WSUS	业务平面IP	8530	TCP	Windows补丁更新。	否	无	无	业务平面	V100R002C02	无	无
WSUS	业务平面IP	随机	微软update网站	业务平面IP	80	TCP	Windows补丁更新。	否	无	无	业务平面	V100R002C02	无	无
WSUS	业务平面IP	随机	微软update网站	业务平面IP	443	TCP	Windows补丁更新。	否	无	无	业务平面	V100R002C02	无	无
ITA	管理平面IP	随机	GE	管理平面IP	7443	TCP	VRM tomcat https端口	否	是	SSL	管理平面	V100R002C02	无	无
ITA	管理平面IP	随机	GE	管理平面IP	7070	TCP	VRM tomcat http端口	否	无	无	管理平面	V100R002C02	无	无
AD	管理平面IP	123	GE	管理平面IP	123	UDP	NTP	否	无	无	管理平面	V100R002C02	无	无
DesktopCloud portal	管理平面IP	随机	GE	管理平面IP	7483	TCP	tomcat https端口 访问DesktopCloud Portal使用	否	是	SSL	管理平面	V100R002C02	无	无
LogGetter	管理平面IP	20、21	GM	管理平面IP	20、21、30000~30100	TCP	FTP，上传备份文件	否	是	SSL	管理平面	V100R002C02	无	无
UserVM	业务平面IP	随机	KMS	业务平面IP	1688	TCP	Windows 7 用户虚拟机激活。	否	无	无	业务平面	V100R002C02	无	无

- 通过防火墙做隔离，开通指定的端口，屏蔽服务器免受攻击。
- 上图所示各服务器必要的端口信息。



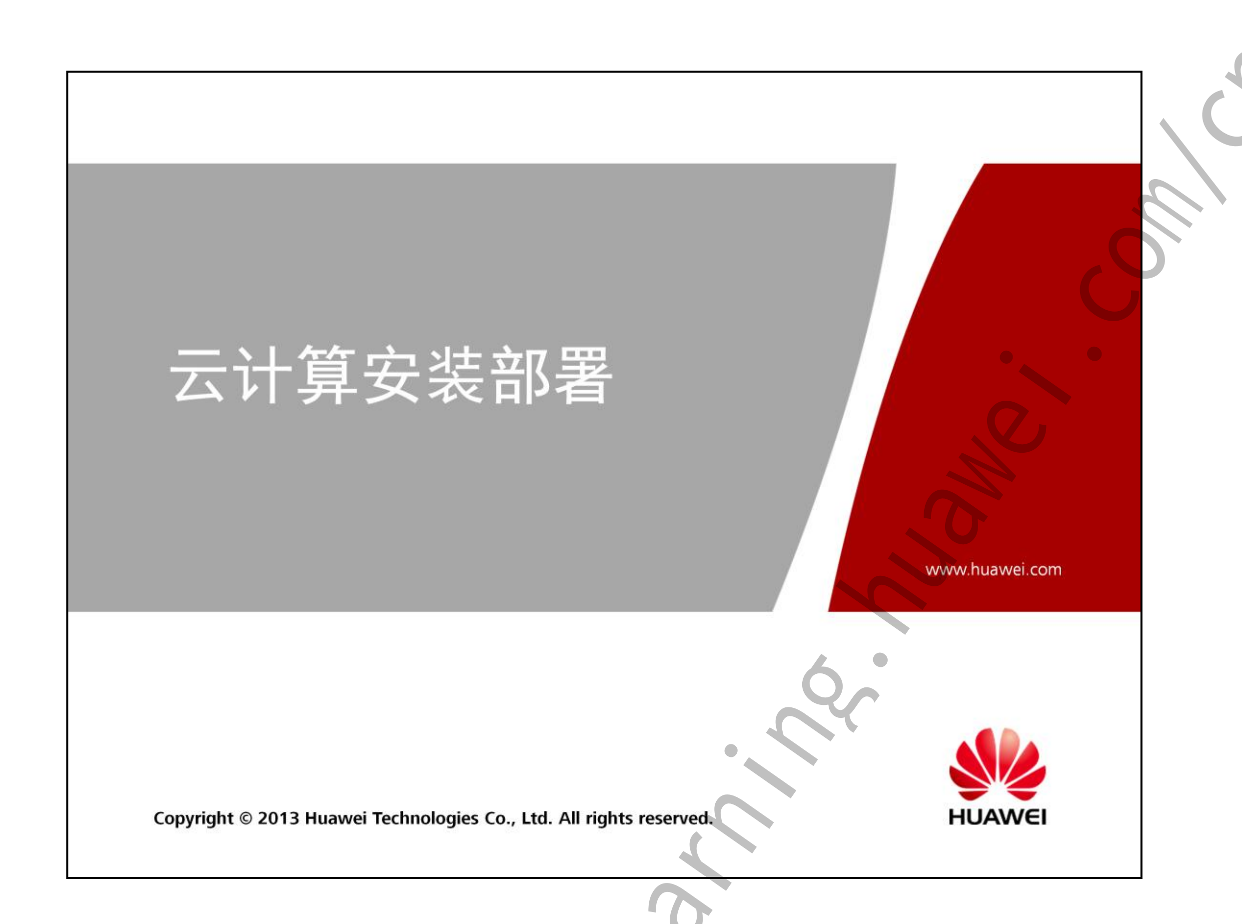
总结

- 云安全基本知识
- 终端及接入安全
- 网络安全
- 虚拟化软件安全
- 数据安全
- 运维安全
- 基础设施安全



Thank you

www.huawei.com


云计算安装部署
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目标

- 学完本课程后，您将能够:
  - 云计算系统总体部署流程
  - 网络规划
  - 服务器规划
  - 存储规划
  - FusionCompute部件的部署
  - FusionManager部件的部署
  - FusionAccess部件的部署
  - 部署验证方法

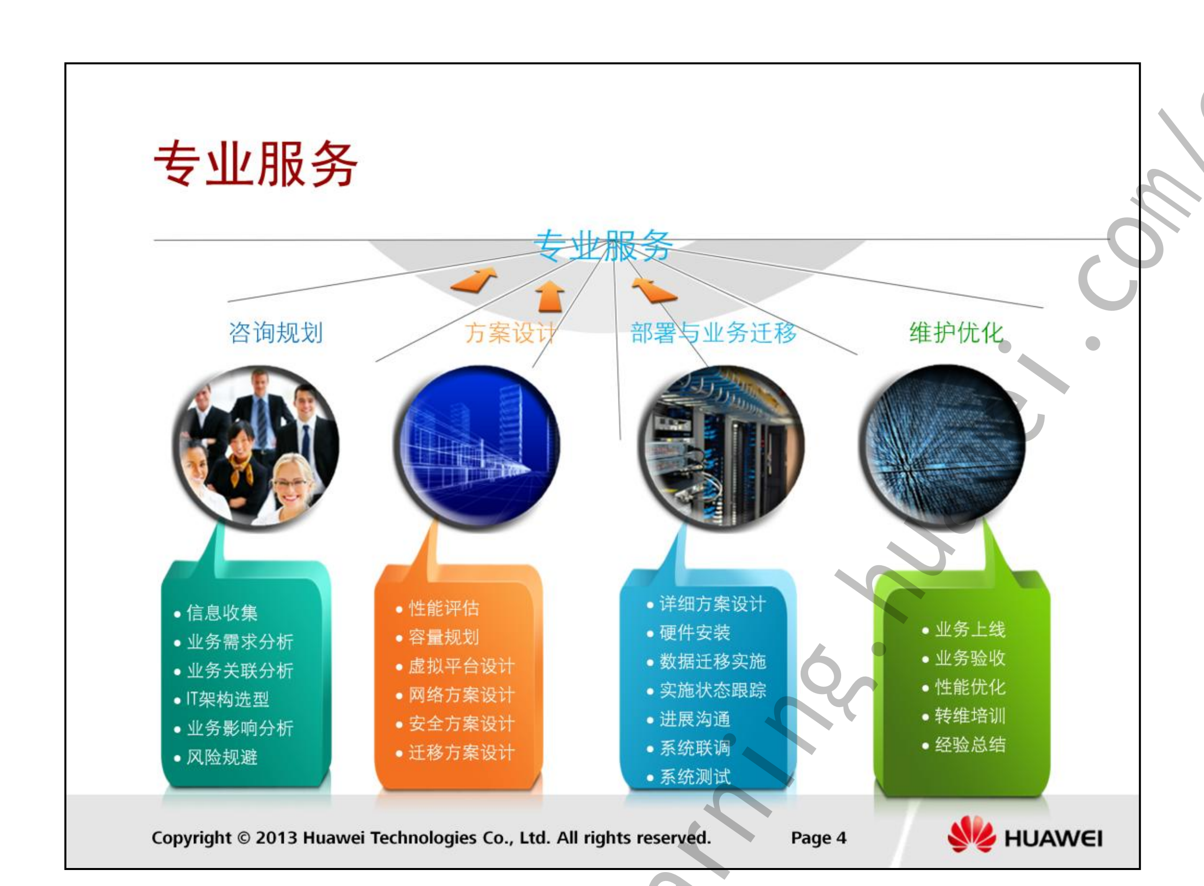




目录

1. **云计算部署流程**
2. 网络规划
3. 服务器规划
4. 存储规划
5. FusionCompute部署
6. FusionManager部署
7. FusionAccess部署
8. 部署验证方法




专业服务
专业服务
咨询规划
方案设计
部署与业务迁移
维护优化
信息收集
业务需求分析
业务关联分析
IT架构选型
业务影响分析
风险规避
性能评估
容量规划
虚拟平台设计
网络方案设计
安全方案设计
迁移方案设计
详细方案设计
硬件安装
数据迁移实施
实施状态跟踪
进展沟通
系统联调
系统测试
业务上线
业务验收
性能优化
转维培训
经验总结
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 4
HUAWEI

专业的服务支撑工具



减少遗漏和出错；盘点设备所需的时间最多缩短15%

收集工作负载的性能指标（CPU/内存/存储IO/网络IO）；软件、硬件、数据资产信息：支撑整合规划、设计、实施及验证。



业务部署合理，资源利用率高

根据当前应用以及性能数据，规划1）VM规格，2）整合策略：3）预测模型。



专业化、高质量的IT架构

根据项目BoQ和物理设计原则，自动完成工程实施所使用的板位图、连线关系表、线缆标签；并提供数据给逻辑设计。



数据、应用、OS资产的继承和利旧

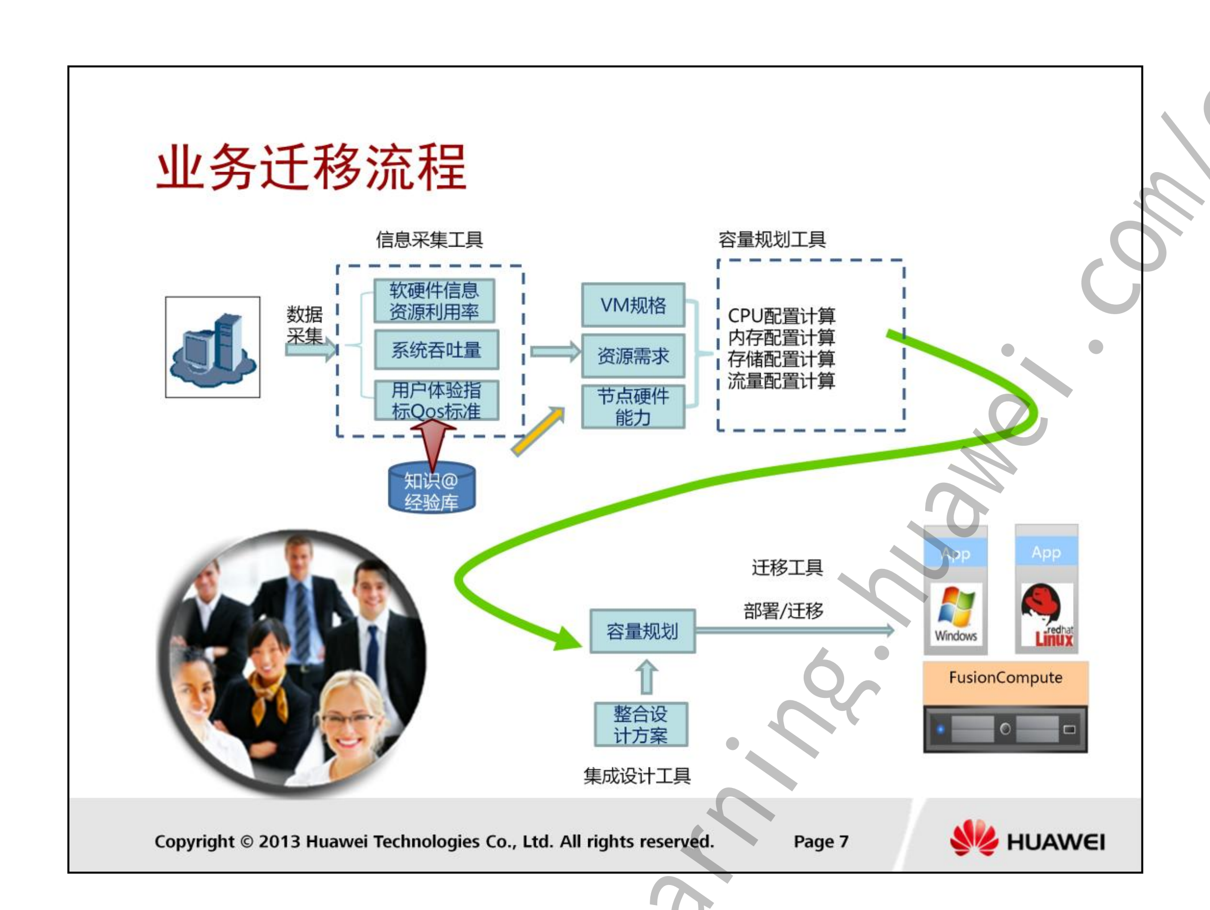
提供P2V/V2V功能，将数据安全的从物理机到虚拟机互相搬迁。

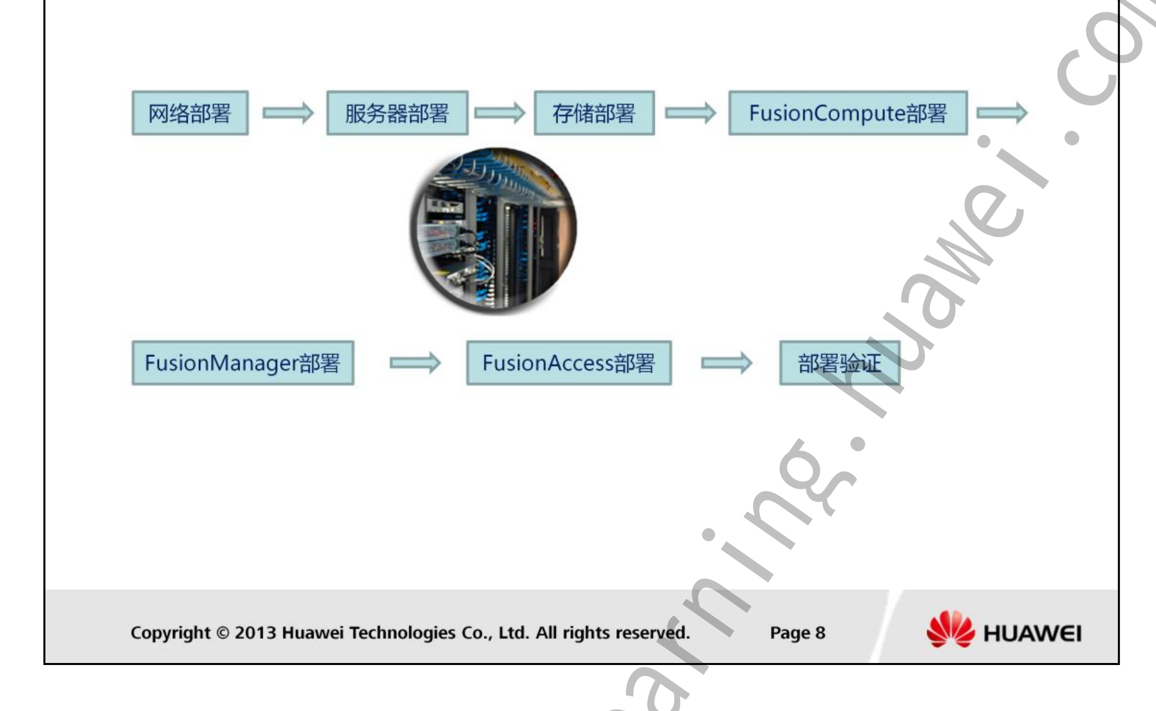






- 迁移服务通过项目逐步积累并丰富知识和案例库。知识和案例库反向作用，提高迁移服务工具化，专业化。
- 汇总项目采集数据，指导咨询服务和新建业务场景容量规划，提高咨询服务和容量规划的专业度。
- 不断总结优化迁移方案和迁移实施过程，提高迁移质量、缩短迁移实施时间和业务停机时间，提高客户满意度。
- 积累业务调优经验，指导后续项目业务优化实施。
- 总结项目管理经验，优化项目交付过程，提高风险识别和应对能力。


业务迁移流程
信息采集工具
容量规划工具
数据
采集
软硬件信息
资源利用率
系统吞吐量
用户体验指
标Qos标准
知识@
经验库
VM规格
资源需求
节点硬件
能力
CPU配置计算
内存配置计算
存储配置计算
流量配置计算
迁移工具
部署/迁移
容量规划
整合设
计方案
集成设计工具
App
App
Windows
redhat
Linux
FusionCompute
Page 7
HUAWEI



- 网络部署
  - 接入层网络部署
  - 汇聚层网络部署
  - 核心层网络部署
  - 广域网网络部署
- 服务器部署
  - 服务器网卡部署
  - 服务器硬盘部署
- 存储部署
  - 存储网络部署
  - 存储RAID部署
- FusionCompute部署
  - 软件安装
  - 初始配置
  - 软件调测
- FusionManager部署
  - 软件安装
  - 初始配置
  - 软件调测
- FusionAccess部署
  - 软件安装
  - 初始配置
  - 终端配置
  - 证书配置
  - 软件调测
- 部署验证
  - 设计验证方案
  - 定制测试用例
  - 实施验证
  - 输出验证报告



目录





目录

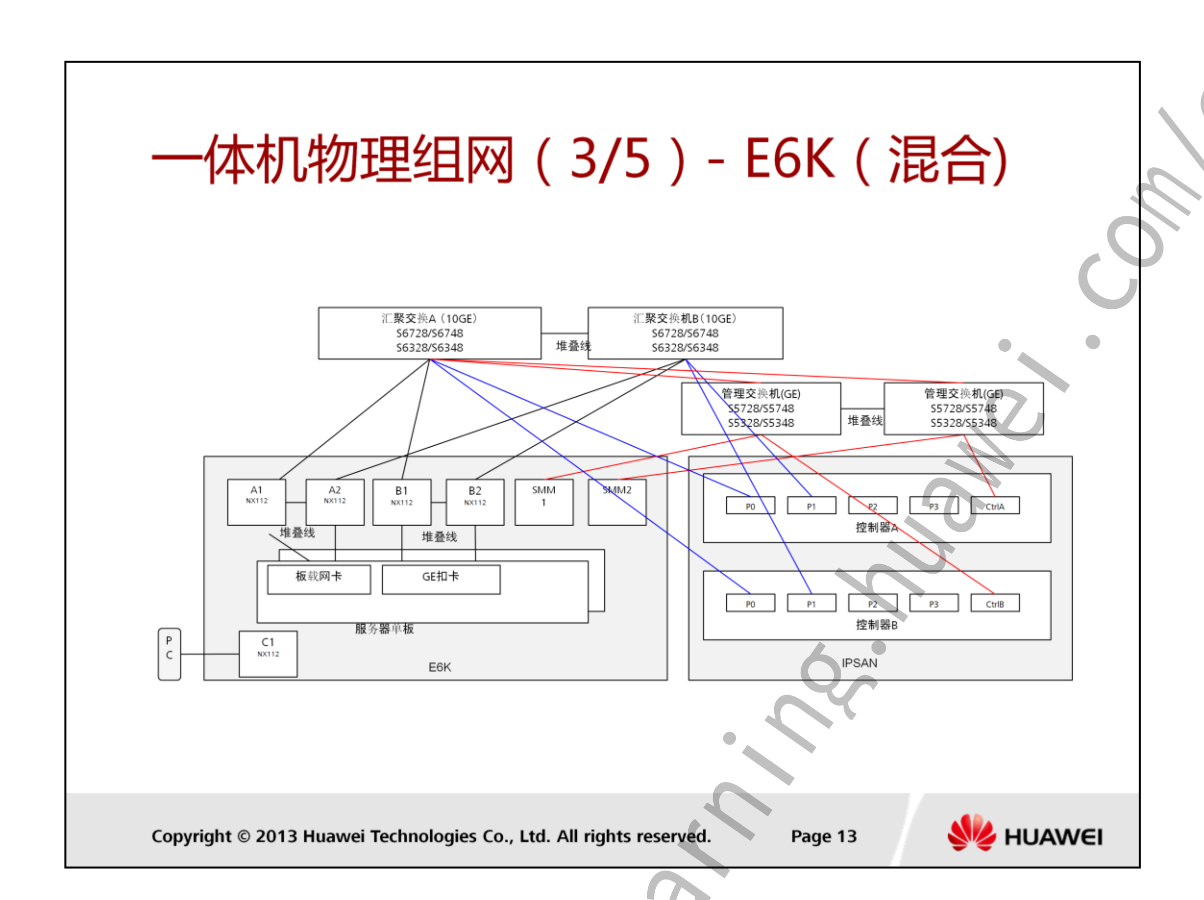


一体机物理组网（1/5）- E6K（1GE）

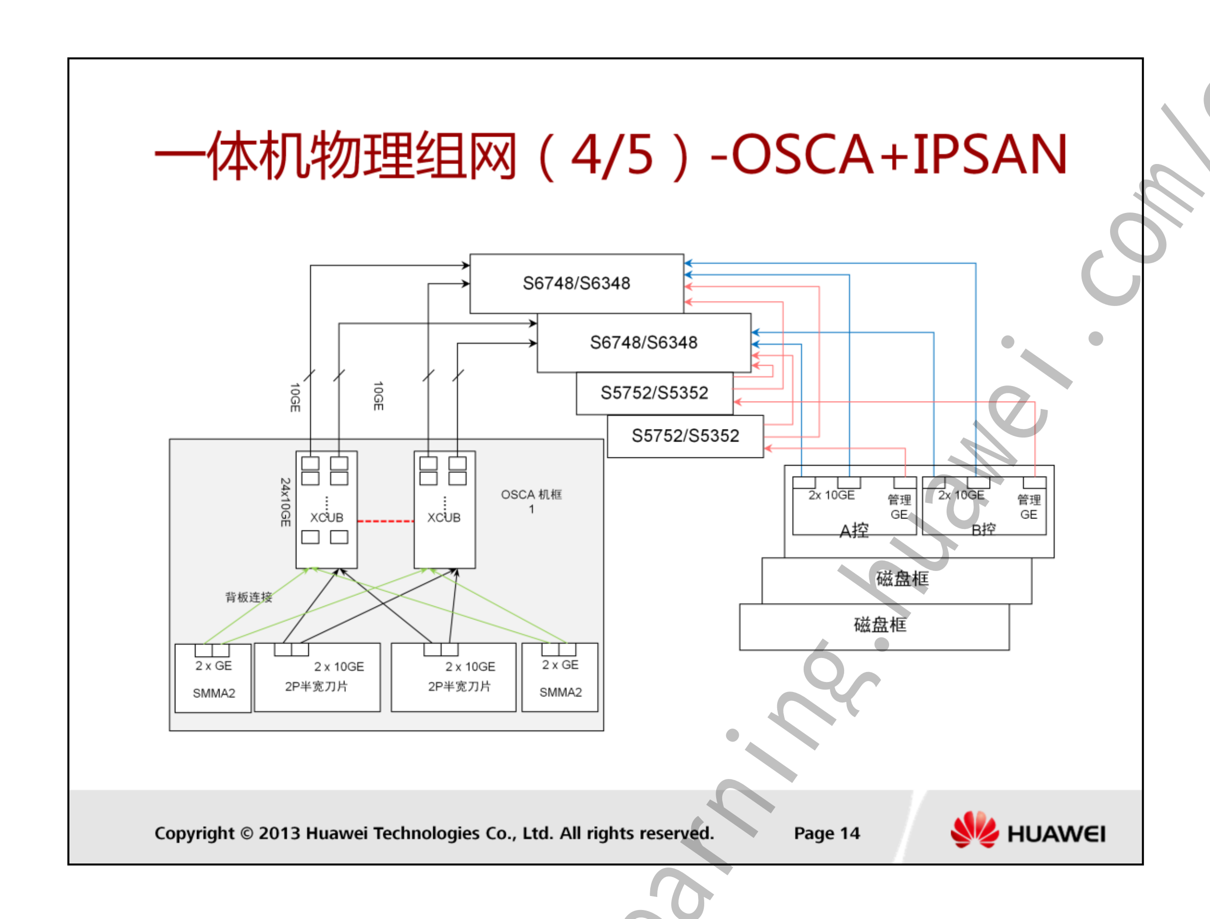
- 1.E6K 服务器单板出4×1GE
- 2.E6K 使用A1、A2、B1、B1 NX112交换机
- 3.外置汇聚交换机使用48口或24口 S53或S57系列GE交换机
- 4.IPSAN 出GE接口连接到外置GE汇聚交换机
- 5.单平面端口需求： E6K 5×1GE， IPSAN 5×1GE；使用S5328可支持2对E6K +2对IPSAN

一体机物理组网（2/5） E6K（10GE）

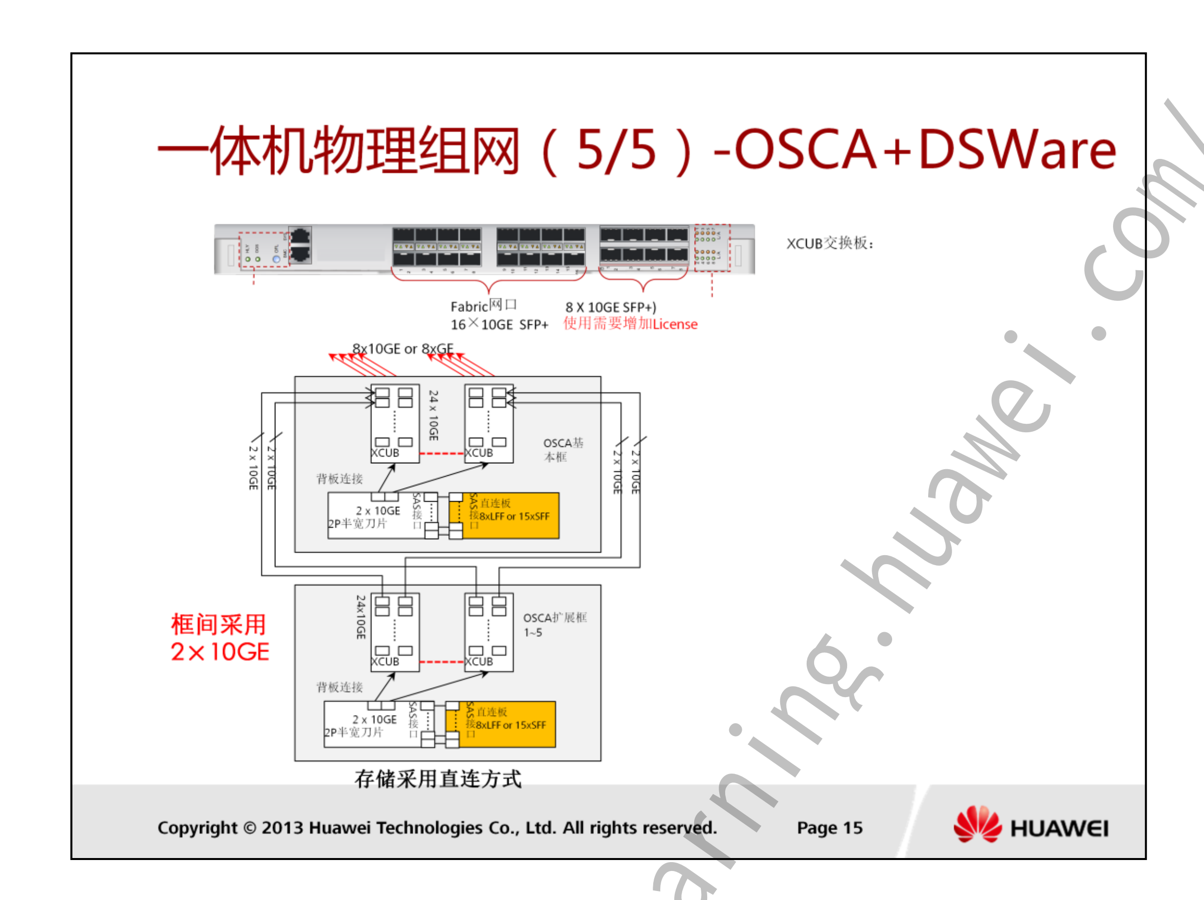
- 1.E6K 服务器单板出4×1GE
- 2.E6K 使用A1、A2、B1、B1 NX112交换机
- 3.外置汇聚交换机使用48口或24口 S53或S57系列GE交换机
- 4.IPSAN 出GE接口连接到外置GE汇聚交换机
- 5.单平面端口需求：E6K 5×1GE， IPSAN 5×1GE；使用S5328可支持2对E6K +2对IPSAN



- 1.服务单板采用4×1GE
- 2.E6K NX112出10GE上行接口

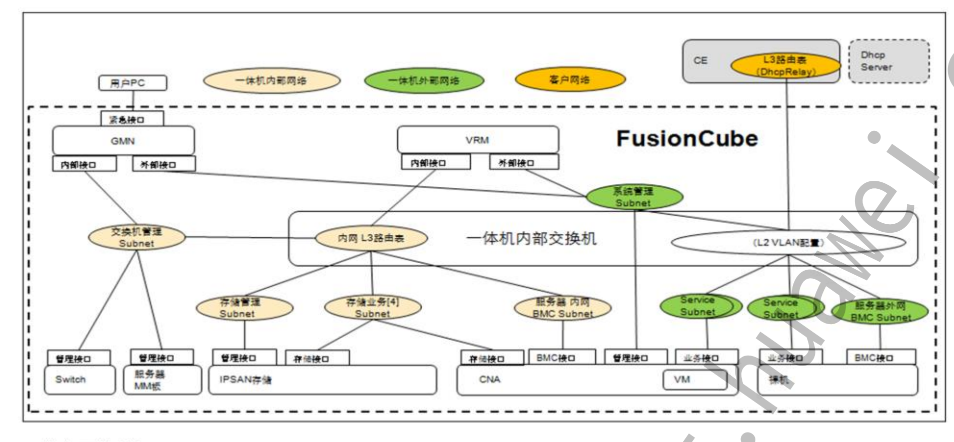


1. OSCA计算
   - 刀片采用2x10GE网卡
   - 交换板采用XCUB，16x10GE，框间单平面出2x10GE
2. IPSAN S5500T
   - 双控，每控制器2x10GE+1GE(管理)
   - 每套IPSAN出4x10GE+2xGE（GE管理口中有SMI-S业务，需要主备提高可靠性）
3. 外置汇聚交换机
   - 1对GE交换机作为IPSAN 管理接入交换机
   - 1对10GE交换机作为业务交换机
   - 48口10GE交换机可级联4框OSCA+6套IPSAN



1. 刀片采用2x10GE网卡
2. 交换板采用XCUB，24x10GE；
3. 基本框作为　　汇聚，单平面上行4x10GE或者4xGE（采用光转电模块）
4. 框间级联单平面4x10GE，最大6框，无预留网口

服务器 + IPSAN 2层模式



一体机网络特点：

1. 一体机网络采用内外网隔离
2. 一体机中交换机、服务（MM板）、存储、单板BMC、CNA存储等IP地址由系统自动分配
3. 一体机中的交换机由系统自动配置；
4. 用户可以通过PC连接FM节点 修改一体机管理IP地址和组网模式；

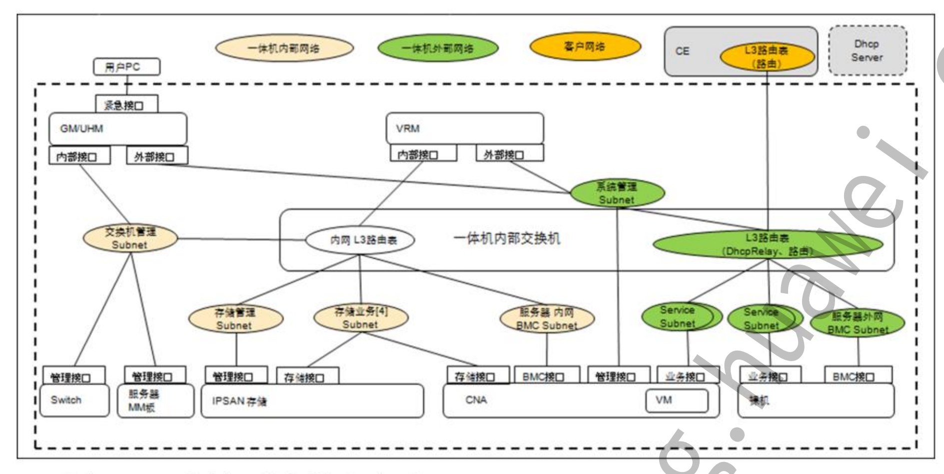


1. 为什么服务器BMC 与存储BMC分开？

A： 动态分配IP地址时，区分计算与存储

2. 为什么 网络设备使用单独Subnet（VLAN）-- 动态分配IP地址

服务器 + IPSAN 3层模式



1. 一体机可采用2层模式或3层模式连接到用户网络
2. 一体机可实现虚拟机IP地址的自动分配， 也可由客户提供DHCP Server或手工配置IP地址
3. 一体机裸机发放时，IP地址由客户提供的DHCP Server或手工进行配置

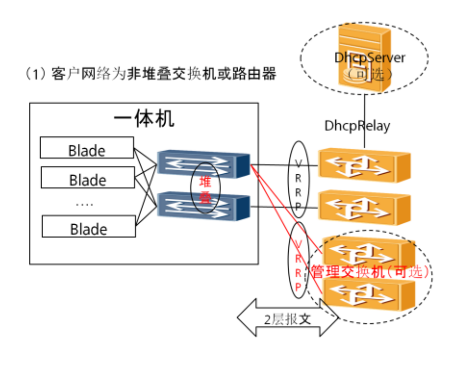


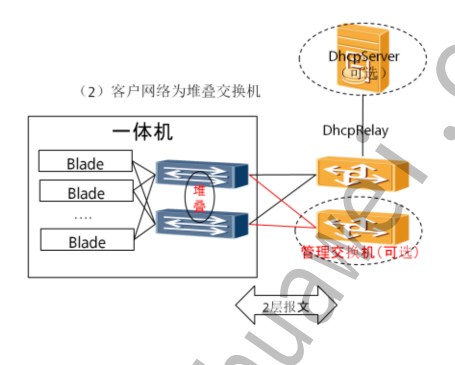
1. 为什么服务器BMC 与存储BMC分开？

A： 动态分配IP地址时，区分计算与存储

2. 为什么 网络设备使用单独Subnet（VLAN）-- 动态分配IP地址

一体机2层模式连接用户网络



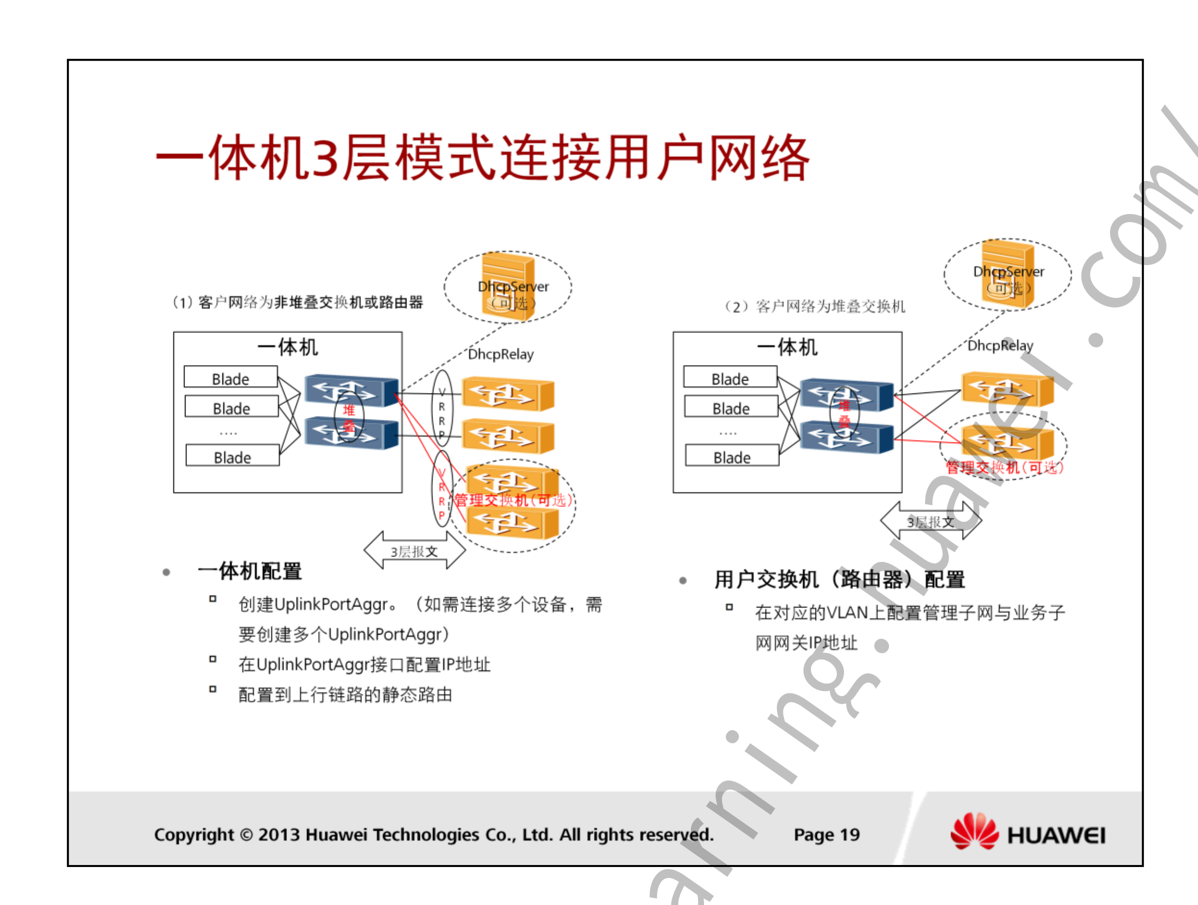




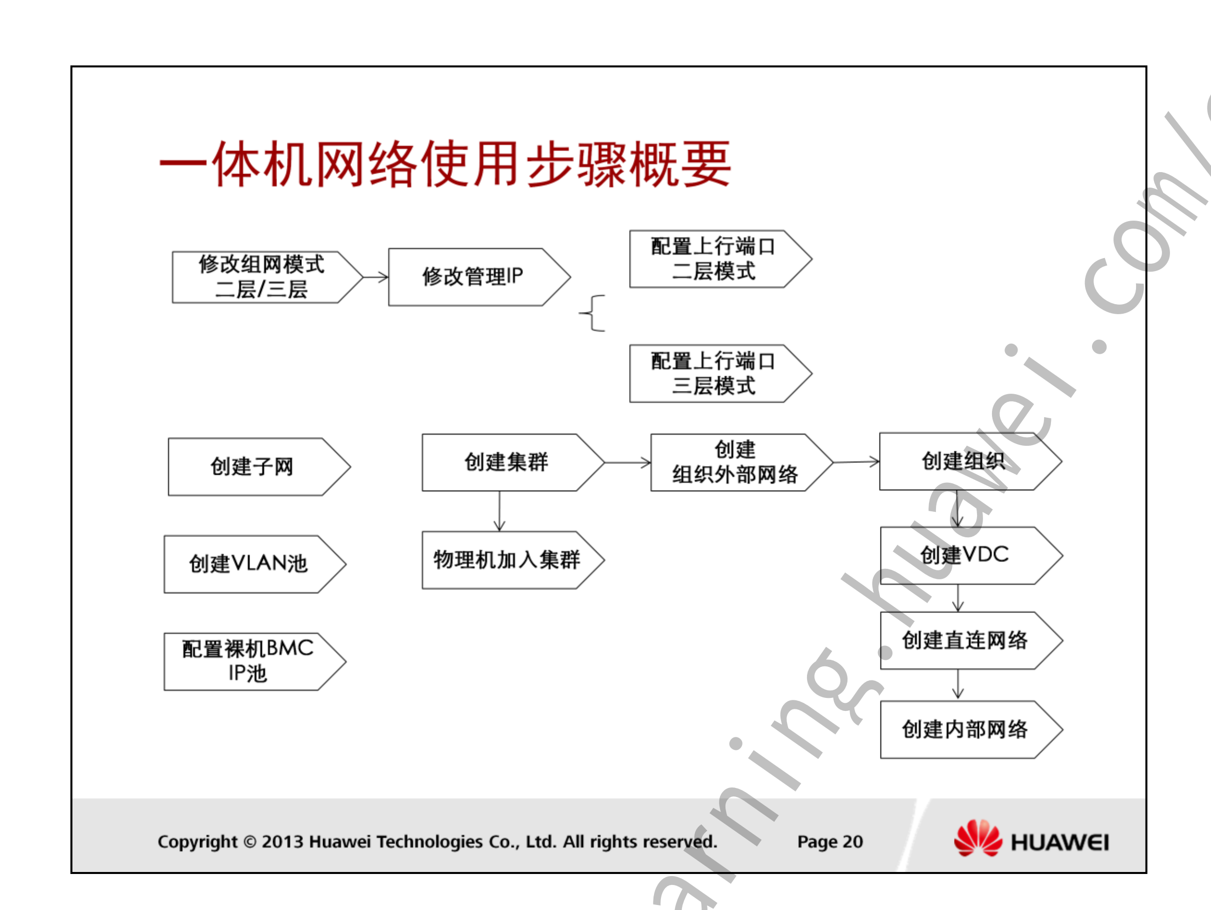
- **一体机配置**
  - 创建UplinkPortAggr。（如需连接多个设备，需要创建多个UplinkPortAggr）
  - Uplink口配置需要通过的VLAN（管理口VLAN与业务口VLAN）
- **用户交换机（路由器）配置**
  - 在对应的VLAN上配置管理子网与业务子网网关IP地址
  - 在业务子网网关配置DHCP Relay
  - 一体机分配IP地址 – Server为VRM IP地址；
  - 用户DHCP分配IP地址 – Server为DHCP

HUAWEI

- 2层模式定义
  - 子网的网关配置客户网络，仅将一体机交换机作为接入交换机
- 应用场景
  - 要求管理与业务隔离；
  - 用户可配置不同子网安全隔离



- 3层模式定义
  - 管理与业务网关配置一体机，用户网络与一体机采用3层路由进行互通；
- 应用场景
  - 减少用户网络，直接采用路由连接到一体机
- 物理配置


一体机网络使用步骤概要
修改组网模式
二层/三层
修改管理IP
配置上行端口
二层模式
配置上行端口
三层模式
创建子网
创建集群
创建
组织外部网络
创建组织
创建VLAN池
物理机加入集群
创建VDC
配置裸机BMC
IP池
创建直连网络
创建内部网络
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 20
HUAWEI

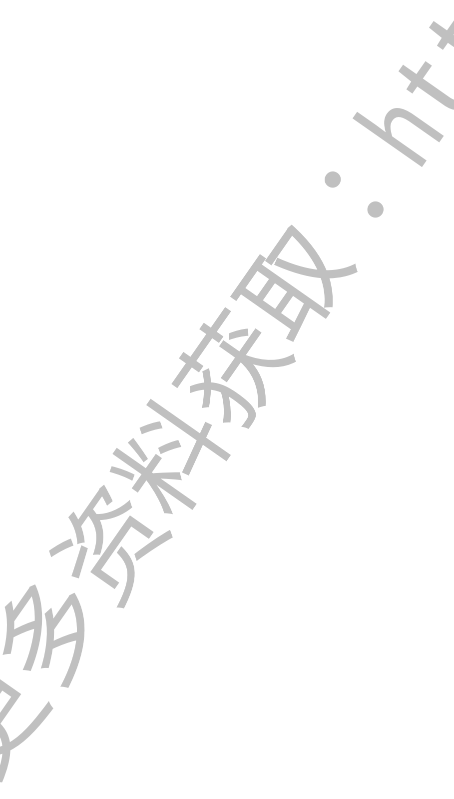
一体机网络使用- 设置网络模式&修改IP





- **通过系统应急接口 连接FM修改网络模式和管理IP**
- **系统默认是三层模式**
- **管理子网至少使用的IP地址个数：**
  - IPSAN存储场景 8个IP， FM(3), VRM(3), MCNA(2)
  - DSWARE存储场景 12个IP， FM(3), VRM(3), DSWARE(3), MCNA(3)





一体机网络使用- 连接用户网络



- **二层模式**

1）创建Uplink聚合端口，

2）选择允许负载均衡算法和允许通过的VLAN

- **三层模式**

1）创建Uplink聚合端口，

2）配置接口IP地址

3）配置静态路由





HUAWEI

一体机网络使用-创建子网与VLAN池

FusionManager 服务目录 应用管理 资源管理 故障管理 系统管理

首页 资源管理 添加VLAN池

当前资源分区：fusioncube_zone

VLAN池信息

* 名称： 由中文字符、字母字符、数字、下划线组成，长度范围是1~64。
* 起始VLAN ID：
* 结束VLAN ID： 输入值为2~4000的正整数。

描述： 长度范围0~1024个字符。

添加 取消

子网	二层模式	三层模式
外部DHCP	不支持	支持
内部DHCP	**支持** **表示由一体机分配IP地址**	支持
无DHCP	不支持	支持 **表示网关配置一体机上，仅裸机使用**



一体机网络使用- 配置裸机BMC IP池



- **裸机BMC IP池：当系统使用E6000服务器时，需要配置裸机BMC IP池，用于向裸机集群分配BMC IP地址**

注： 1－二层模式， 需要在用户交换机（路由器)配置BMC 子网的网关；

2- 三层模式， 需要在用户交换机配置到BMC子网的路由



一体机网络使用-外部网络



- **External-Network表示组织的外部网络，可以被不同组织共享**
- **创建外部网络时，可选择：**
  - 使用的子网或VLAN
  - 网络Qos属性：上限带宽，优先级
  - 安全属性：DHCP隔离、IP-MAC绑定



一体机网络使用- 组织网络







- 组织的外部网络：不同组织可以引用相同外部网络
- 创建组织内部网络时，直接选择已经创建好的外部网络

- 组织的内部网络，组织独享的网络
- 创建组织内部网络时，可选择：
  使用的子网或VLAN
  网络Qos属性：上限带宽，优先级
  安全属性：DHCP隔离、IP-MAC绑定





目录

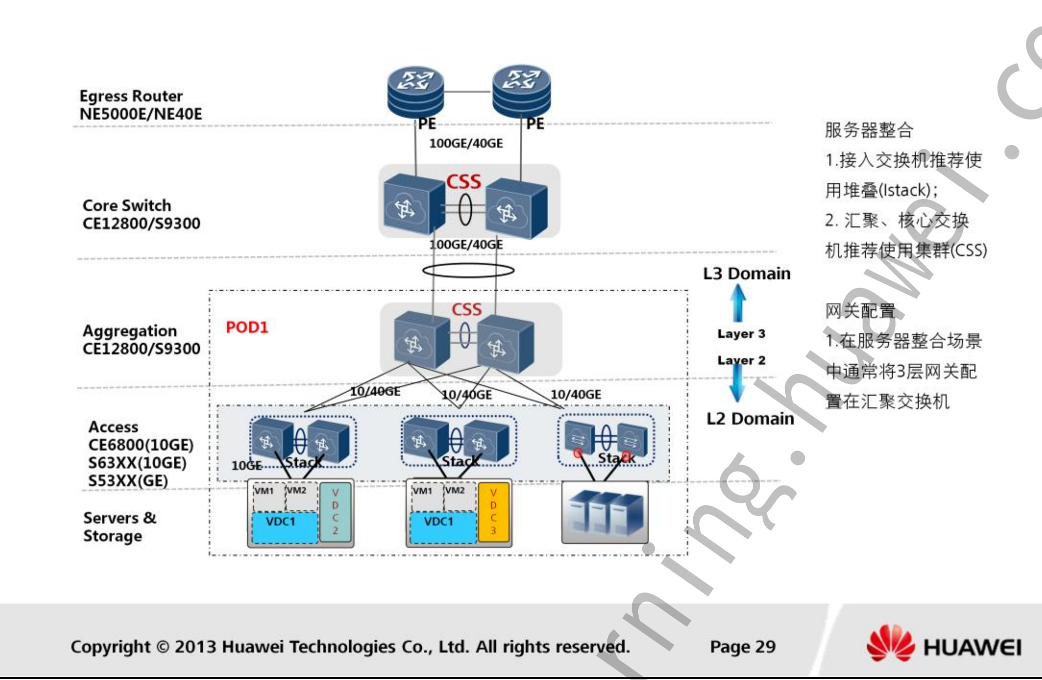




目录



物理网络设备



服务器整合

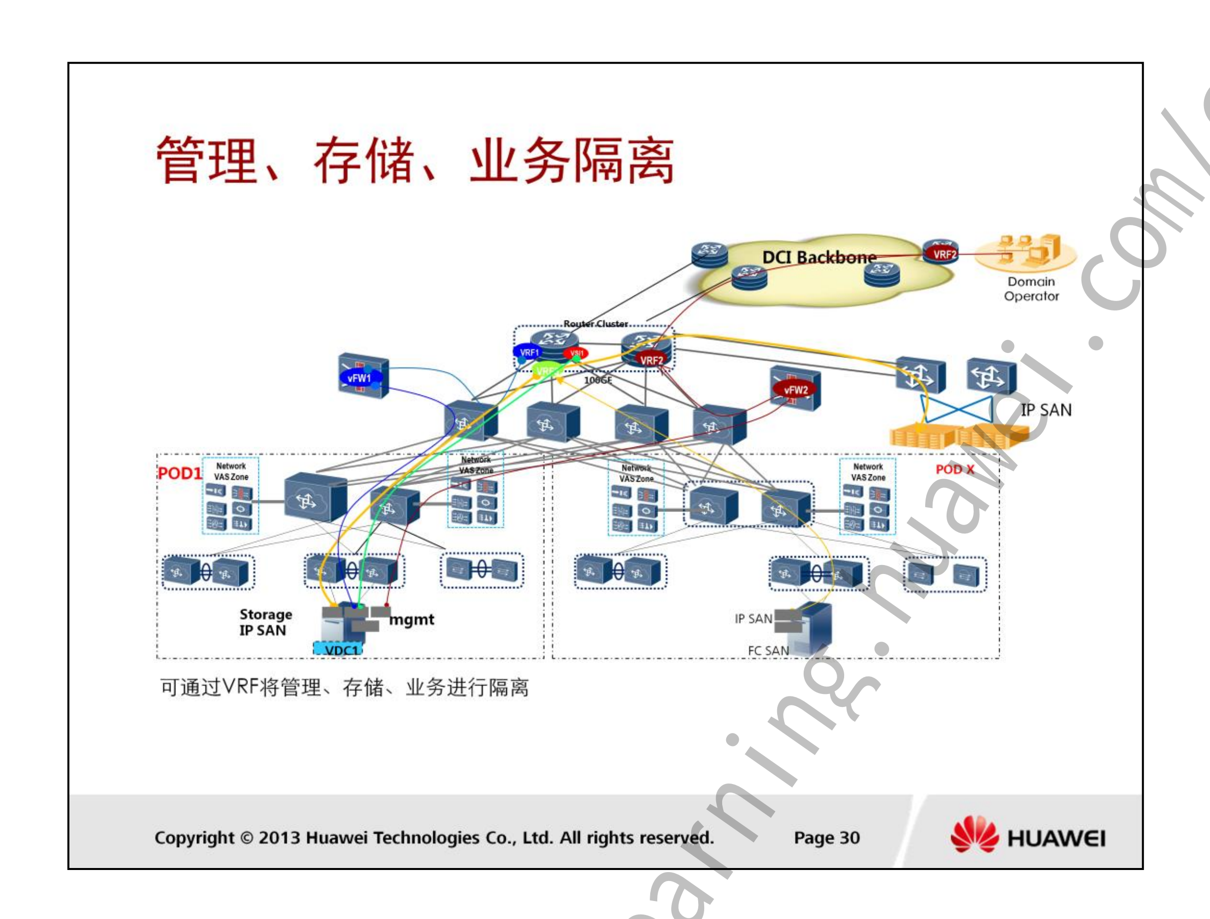
1.接入交换机推荐使用堆叠(Istack)；

2. 汇聚、核心交换机推荐使用集群(CSS)

网关配置

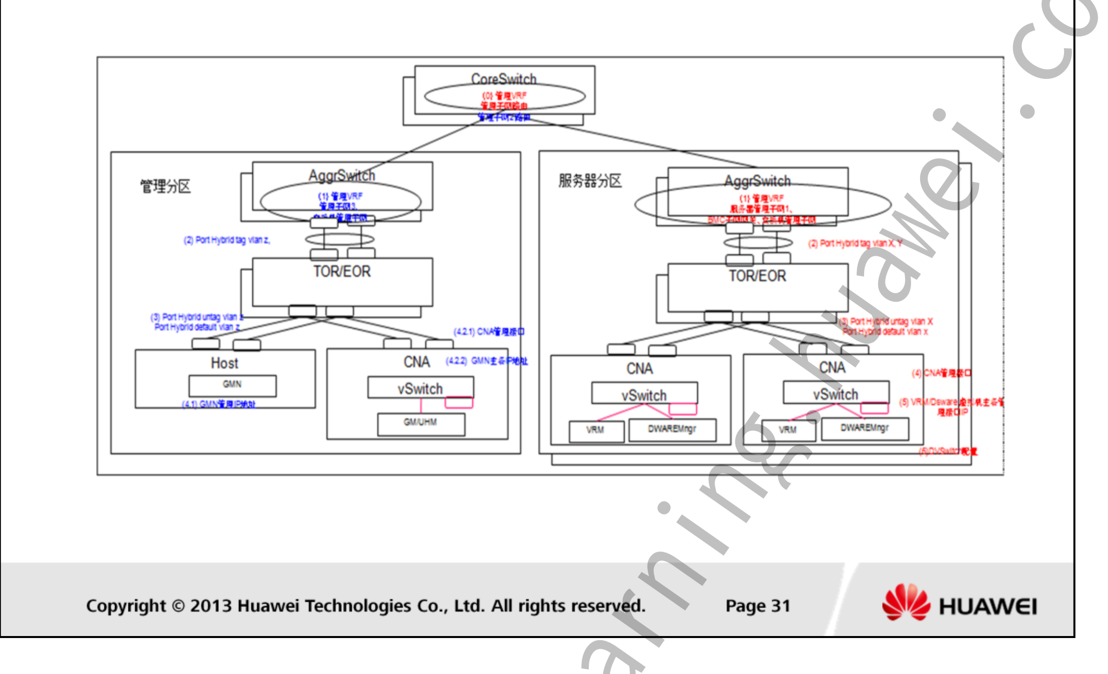
1.在服务器整合场景中通常将3层网关配置在汇聚交换机

HUAWEI



- R3C00 约束-
  1. 虚拟机IP地址由VRM进行分配时，需要业务与管理平面DHCP可互通；
  2. FM AME 功能需要管理平面与业务平面互通才能自动安装应用；

管理平面网络配置



- **管理节点物理部署形式：**

  1）管理分区与服务器分区合一部署

  2）管理分区与服务器分区分离部署

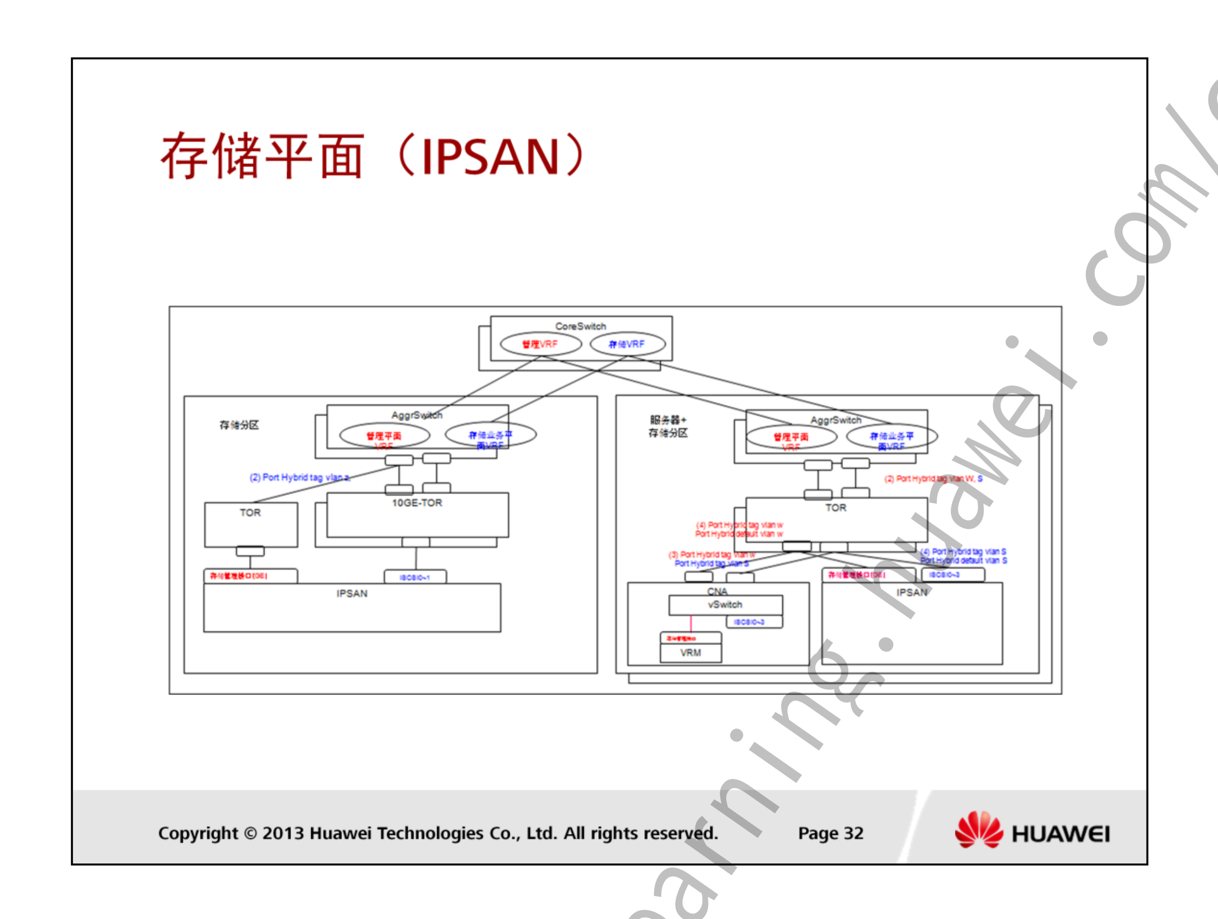
- **管理与业务隔离形式：**

  1）管理与业务隔离（带外）

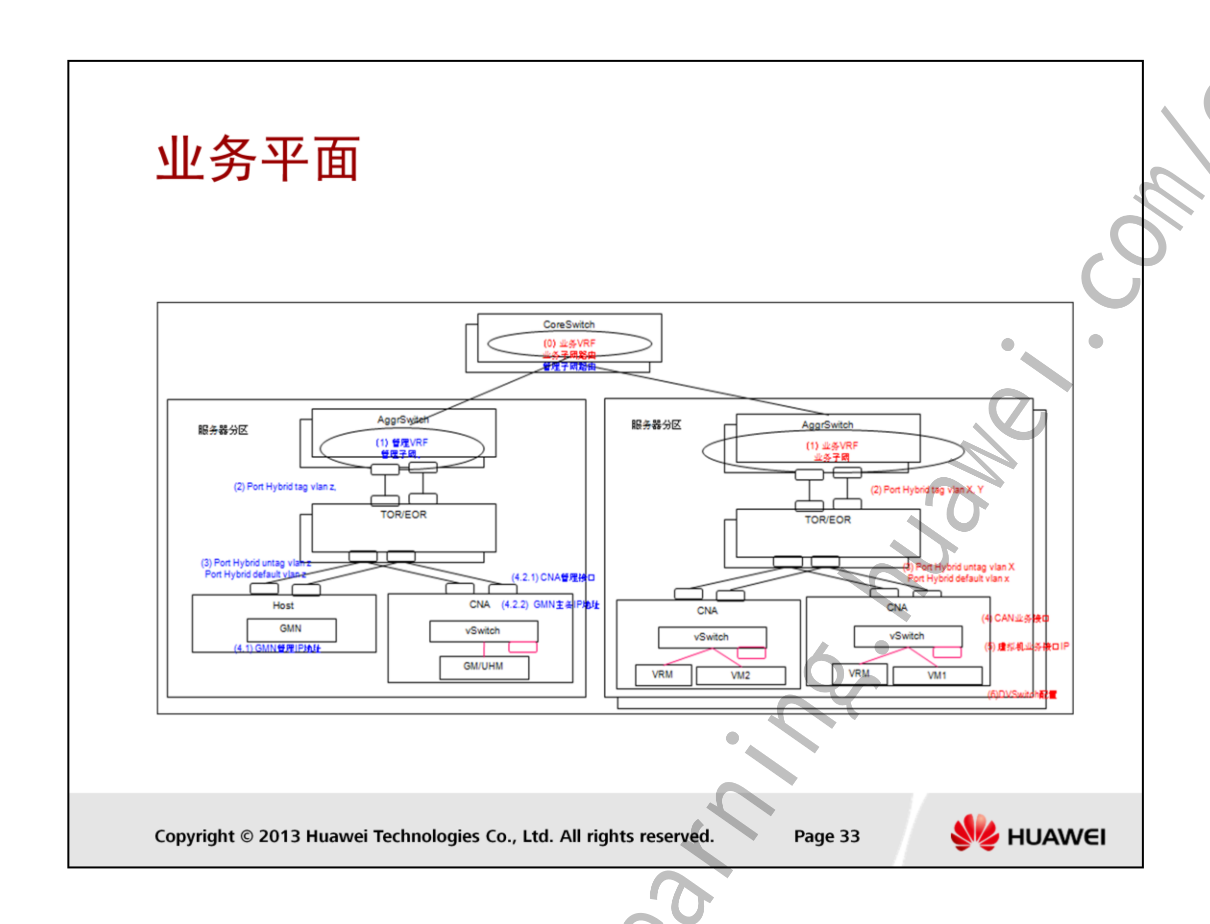
  备选1：FM 与VM 间部署Firewall，配置ACL过滤规则

  备选2：FM 采用独立的业务接口与VM进行通信

  2）管理与业务融合（带内）



1. IPSAN可与服务器部署在服务器分区或部署在独立的存储分区中；
2. 根据存储负载要求采用10GE IPSAN或GE IPSAN。当采用10GE IPSAN时， 需要部署GE交换机连接IPSAN管理接口；
3. 采用GE接口组网， 可将存储与业务分离，采用不同的物理接口；



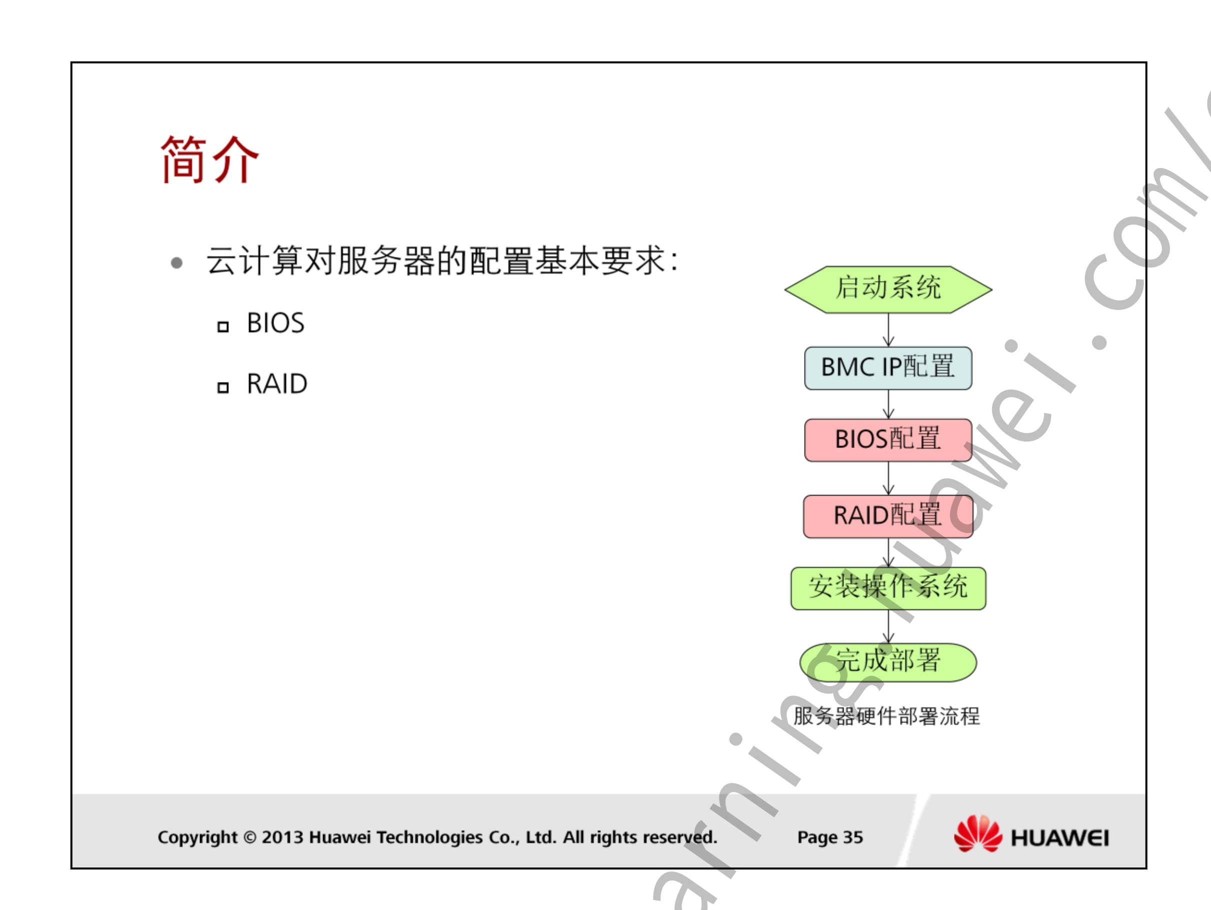
1.采用外部DHCP Server时， 需要E2E保证 汇聚交换机与业务子网网关地址路由可达

2.采用系统内部DHCP（VRM）时，需要保证业务VRF到管理VRF的DHCP报文路由可达

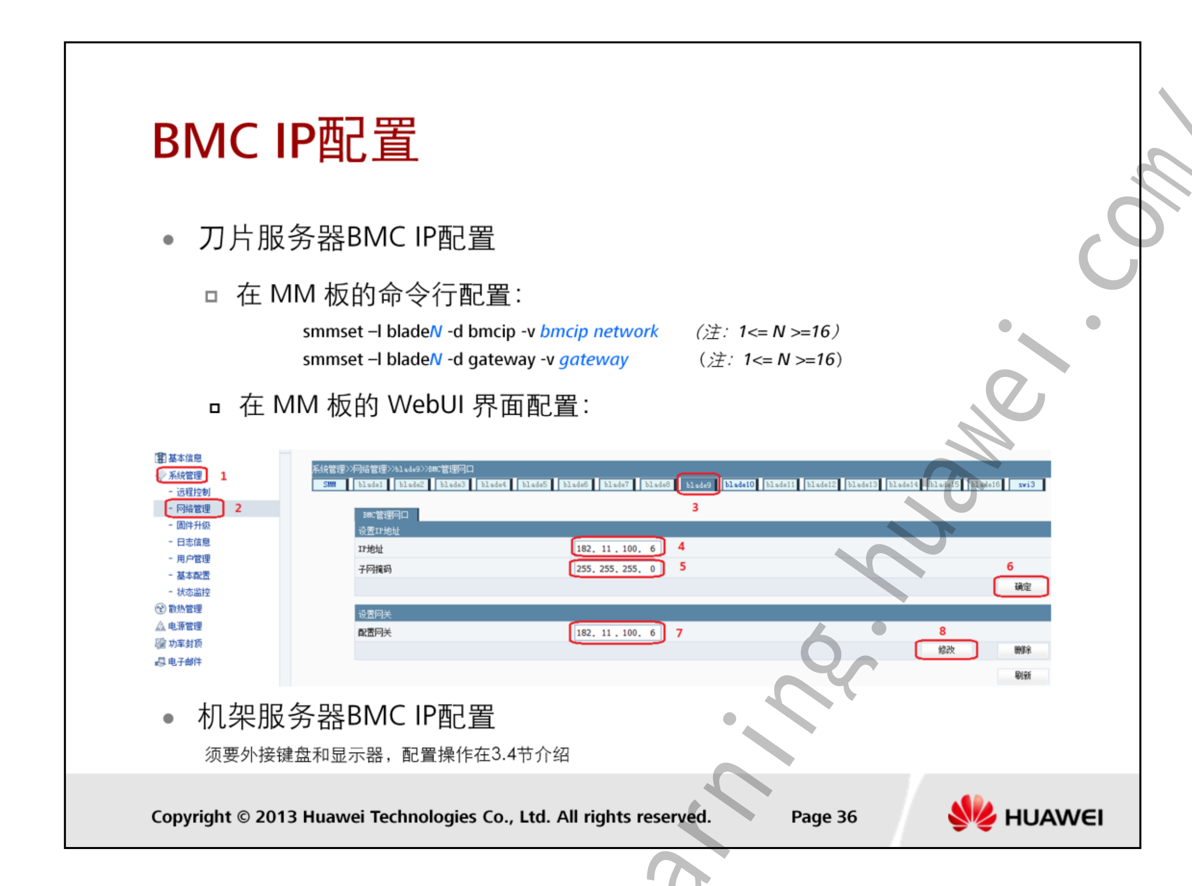


目录





- 服务器硬件部署流程是：服务器系统上电-> 配置 BIOS -> 配置RAID -> 安装操作系统
- 配置BMC IP地址的方式与服务器类型有关：刀片服务器可以通过 MM 板的命令行或者 MM 板的 WebUI 界面配置，机架服务器的 BMC IP须要通过外接键盘和显示器在 BIOS 中配置
- 在手动部署服务器硬件时，配置BIOS 和 RAID配置 没有严格的顺序，也可以先配置RAID，后配置BIOS
- 云计算对服务器基本配置是 BIOS 和 Raid，本章节就以 BIOS 和 Raid 卡的必要配置为例，说明配置的操作方式



- 登录 MM 命令行的方式：

　　1、如果 MM 板已经有IP地址，且可以正常连接，则可以通过 ssh 或者 telnet 方式登录到 MM 板的命令行

　　2、如果 MM 板没有 IP 地址，则须要通过串口线连接 MM 板的串口，登录到 MM 板的命令行

- 登录 MM WebUI 界面的方式：

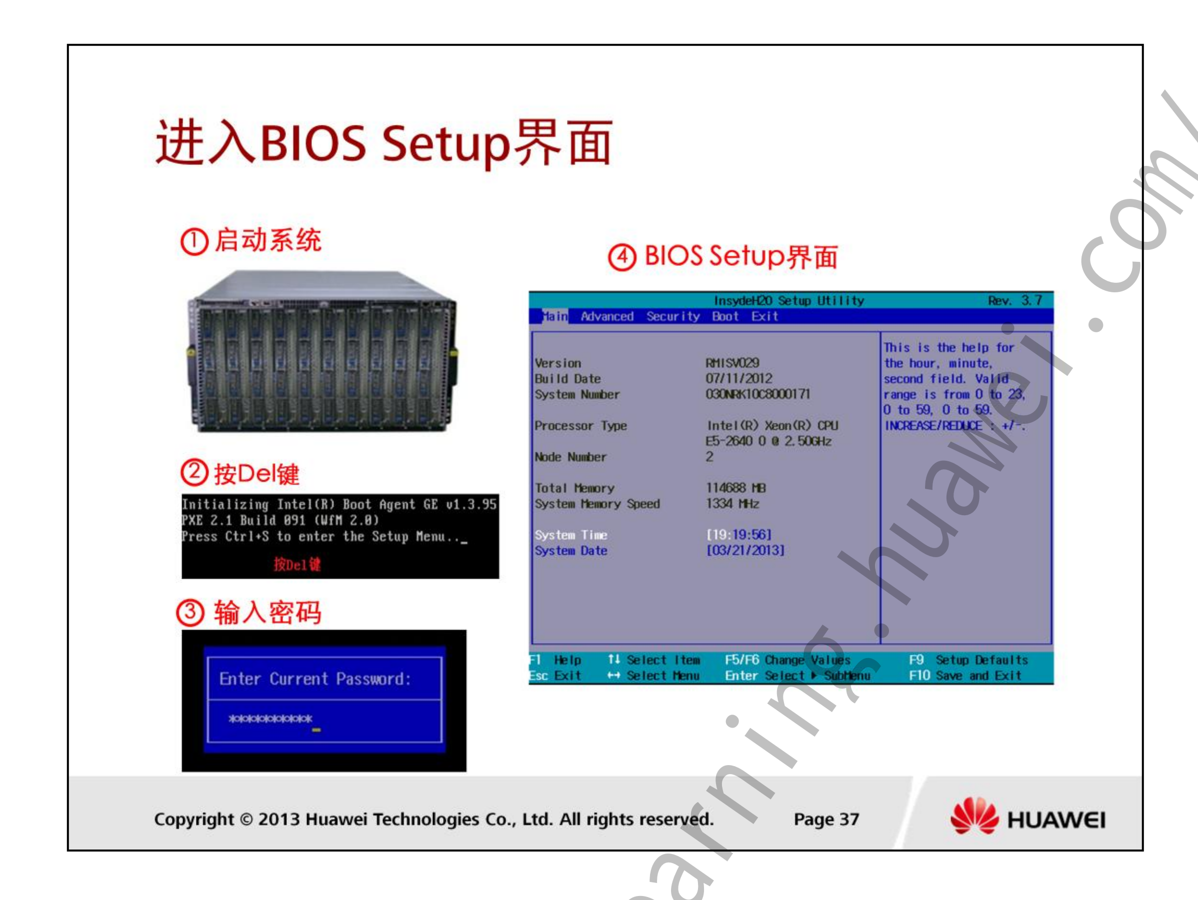
　　1、在浏览器地址栏中输入 MM 板的 IP 地址（前提是 MM 板已经有可用的 IP 地址）

　　2、在出现的界面中输入 MM 的管理员用户名和密码（如：用户名 root，密码 Huawei12#$）

　　3、在登录后的界面中，选择“系统管理”->“网络管理”，在右边的界面中选择目标槽位号

- **说明：**

BMC IP配置是BIOS配置和Raid配置的辅助操作，如果BMC 已经有可用的 IP 就不用配置



- 配置 BIOS，可以快速的按预设的方式安装或者启动操作系统，并且使应用软件能够发挥最佳性能
- BIOS 可以是手工配置，配置前先要进入 BIOS Setup 界面，操作步骤如下：

  1、启动服务器系统

  2、在 BIOS 界面提示“Press Del Enter Setup”时或者在 POST/BIOS 运行的过程中按 Delete键（或者 Del键）　注：Del键按下后放开为一次按键，不能一直长时间按着不放

  3、POST/BIOS 运行完毕后会出现输入BIOS密码的界面，输入BIOS的默认密码（uniBIOS123）就会进入 BIOS Setup 界面

- 启动系统是指让服务器的系统重新运行一次
- BIOS 的操作需要物理显示器和键盘，或者是 BMC 提供的 KVM 功能

BMC 提供的 KVM 功能是要先用浏览器连接 BMC WebUI，然后进入 KVM 界面，方法：

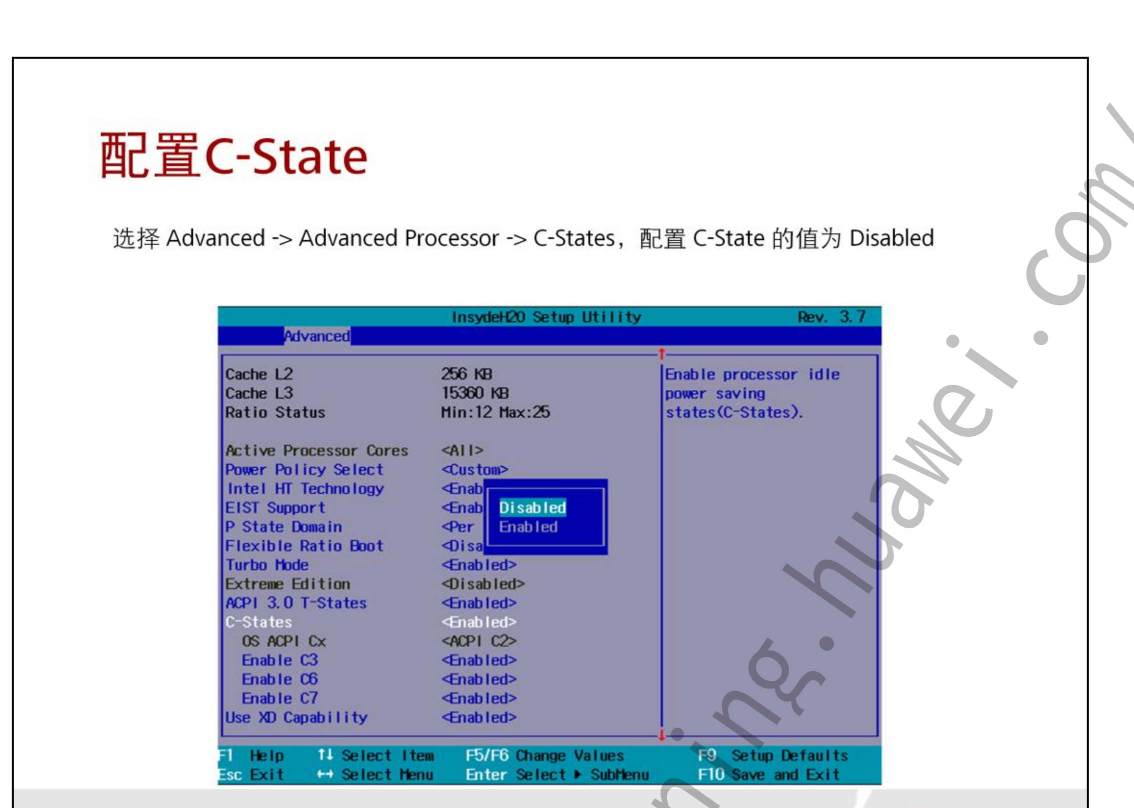
1、打开浏览器

2、输入 BMC IP

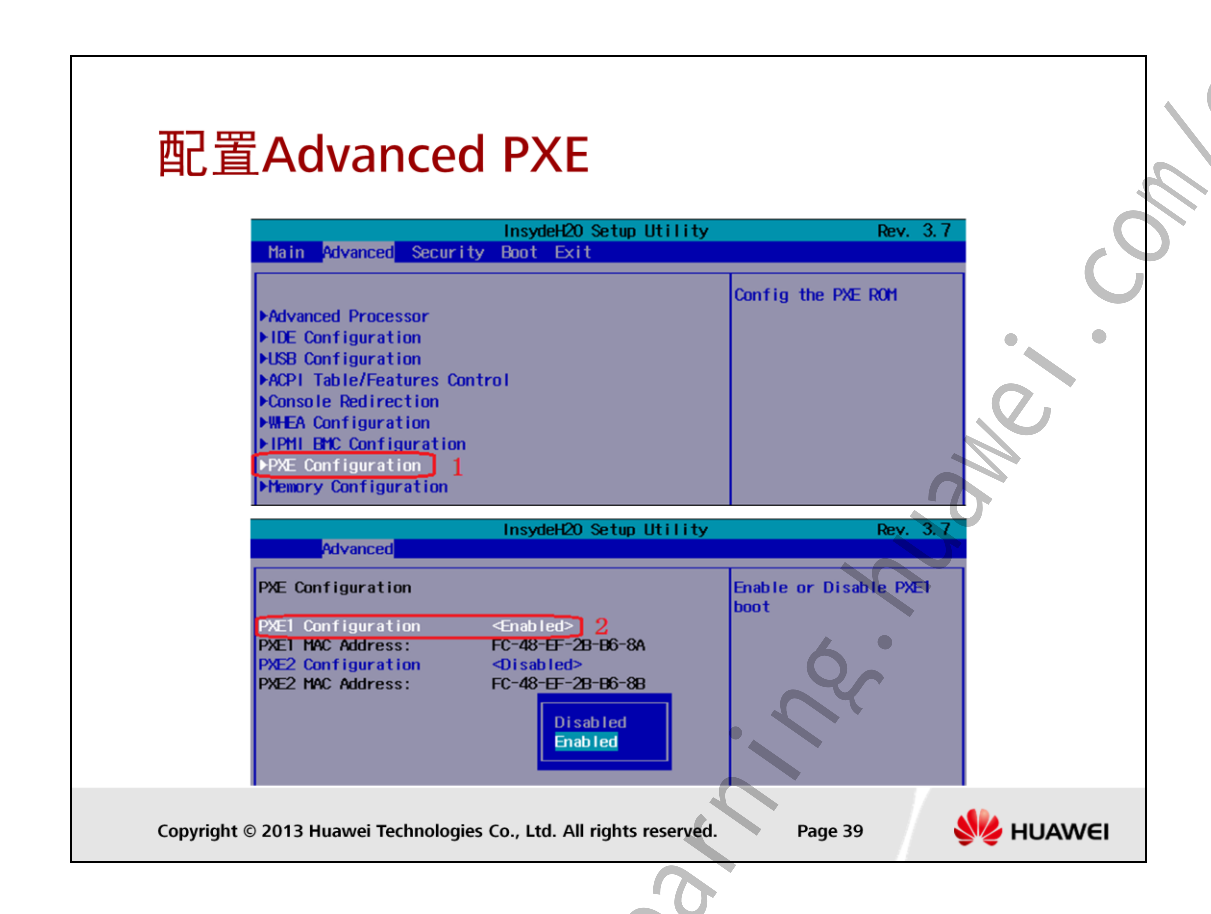
3、输入 BMC 的用户名和密码，登录BMC Web

4、点击界面左侧的“远程控制”链接

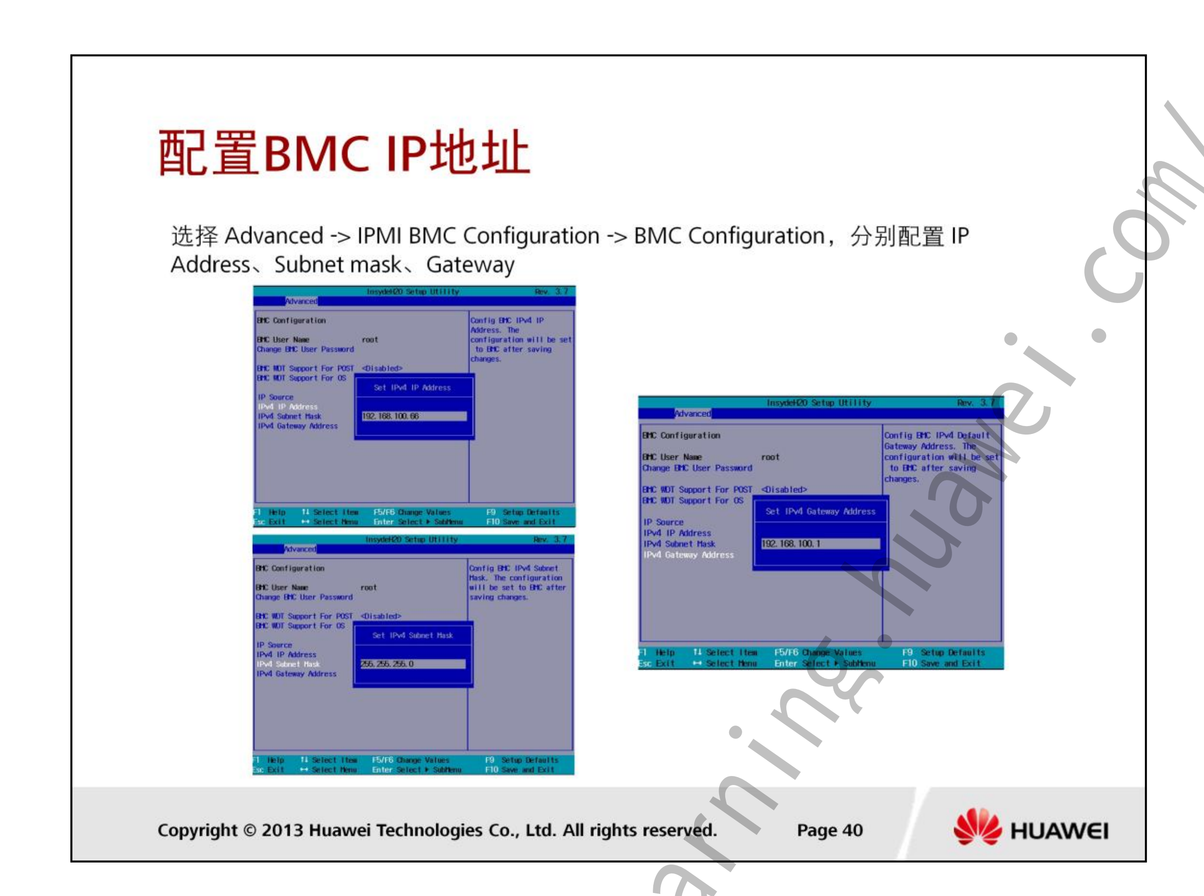
KVM的操作方式如同本地的显示器和键盘



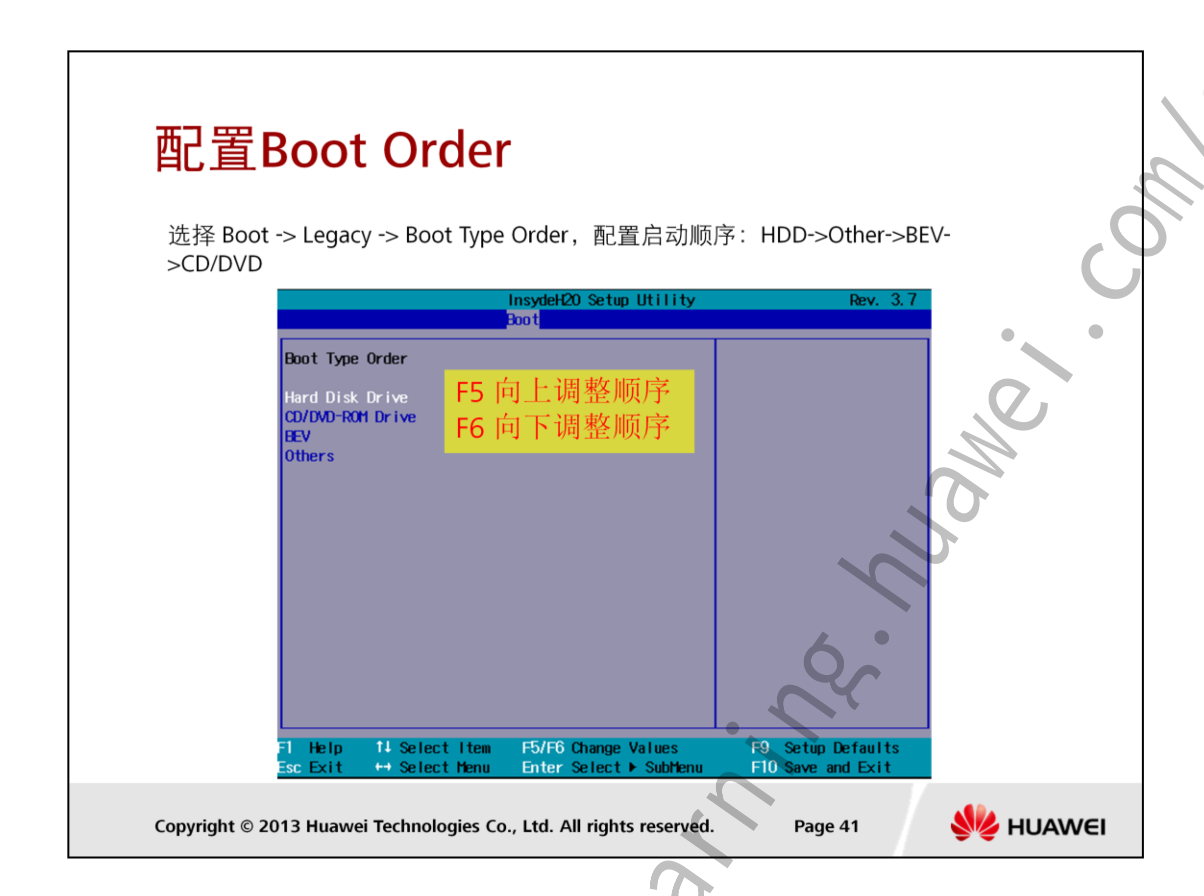
- 服务器的 BIOS 有初始的默认值，修改配置项是为了适应云计算的方案
- 修改 BIOS 的配置需要谨慎
- 配置 BIOS 是修改或者核对配置项的值是否符合要求



- PXE的选项云计算要求第一个网口（PXE1）必须处于使能状态（Enabled），第二个网口一般是禁用状态（Disabled）
- 配置PXE服务可以方便通过网络安装服务器安装操作系统



- 选择配置项后，按回车键，就会出现配置输入框
- 默认网关和子网掩码都是须要配置的项
- 要配置项的值输入完成后，按回国键即可生效，即BMC 的IP信息马上被改变



- BootOrder是一个特殊配置项，表示配置系统启动顺序，默认启动顺序是：BEV，Hard Disk, CD DVD, Other
- 云计算要求配置系统的启动顺序是：Hard Disk, Other, BEV, CD DVD



- BIOS 配置完毕后需要保存才会生效，保存配置的方法：

  1、按快捷键 F10，然后确定，就会保存并自动重启系统

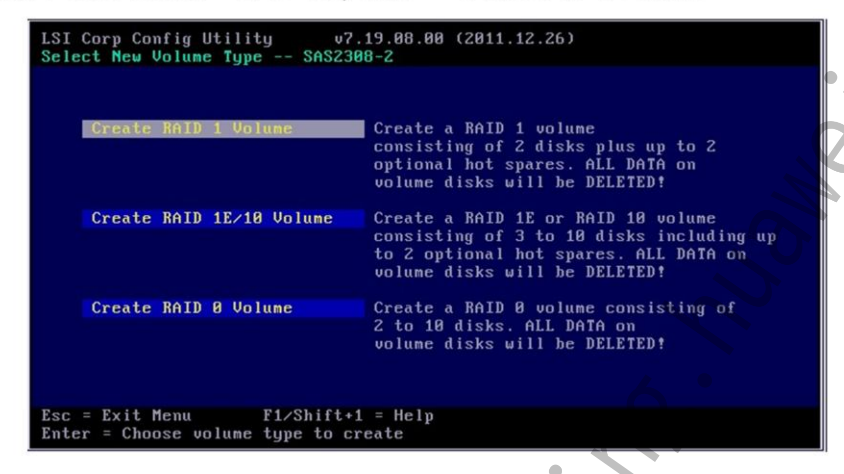
  2、选择Exit -> Exit Saving Changes，按回车键，，就会保存并自动重启系统



- 配置RAID1，可以提高硬盘数据的安全性，如果其中一块硬盘出现故障，另一块硬盘已经百分百的备份了原数据，不怕数据丢失
- 启动系统与配置 BIOS 时启动系统操作相同
- 当 BIOS 出现 “Press Ctrl-C” 时，从键盘上输入 Ctrl+C 组合键，BIOS 就会引导 LSI 的配置界面
- 在配置界面需要确认LSI 扫描到的硬盘是否正确，如硬盘的个数和容量大小
- 配置 Raid 未完成前系统不能下电或者重启

配置Raid

选择：LSISAS2308 -> RAID Properties -> Create RAID 1 Volume





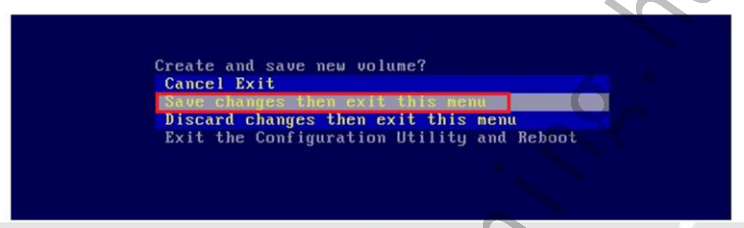


配置Raid(续)

选择加入Raid1 的硬盘，这里只有2块



按 C 键创建Raid1，进入下面界面





配置Raid(续)

Raid1 的配置信息

```
LSI Corp Config Utility        v7.19.08.00 (2011.12.26)
View Volume -- SAS2308-2
       Volume                        1 of 1
       Identifier                    LSI     Logical Volume  3000
       Type                          RAID 1
       Size(GB)                      464
       Status                        Optimal
       Task                          None

      Manage Volume

Slot  Device Identifier              RAID  Hot   Drive       Pred  Size
Num                                  Disk  Spr   Status      Fail  (GB)
  0   ATA     ST9500530NS     SN04   Yes   No    Primary     No     464
  1   ATA     ST9500530NS     SN04   Yes   No    Secondary   No     464

Esc = Exit Menu        F1/Shift+1 = Help
Enter=Select Item   Alt+N=Next Volume
```

连续按3次 ESC 键，选择 “Exit the Configuration Utility and Reboot”



- Raid1配置成功后会返回到Raid卡属性界面，选择“RAID Properties”，就会显示 Raid1的配置信息，这里显示了卷的数量（1），Raid类型（RAID1），卷大小（这里是464GB），硬盘数量（2块），主盘和从盘
- 连续按3次 ESC 键，选择“Exit the Configuration Utility and Reboot”，RAID1 配置结束



目录

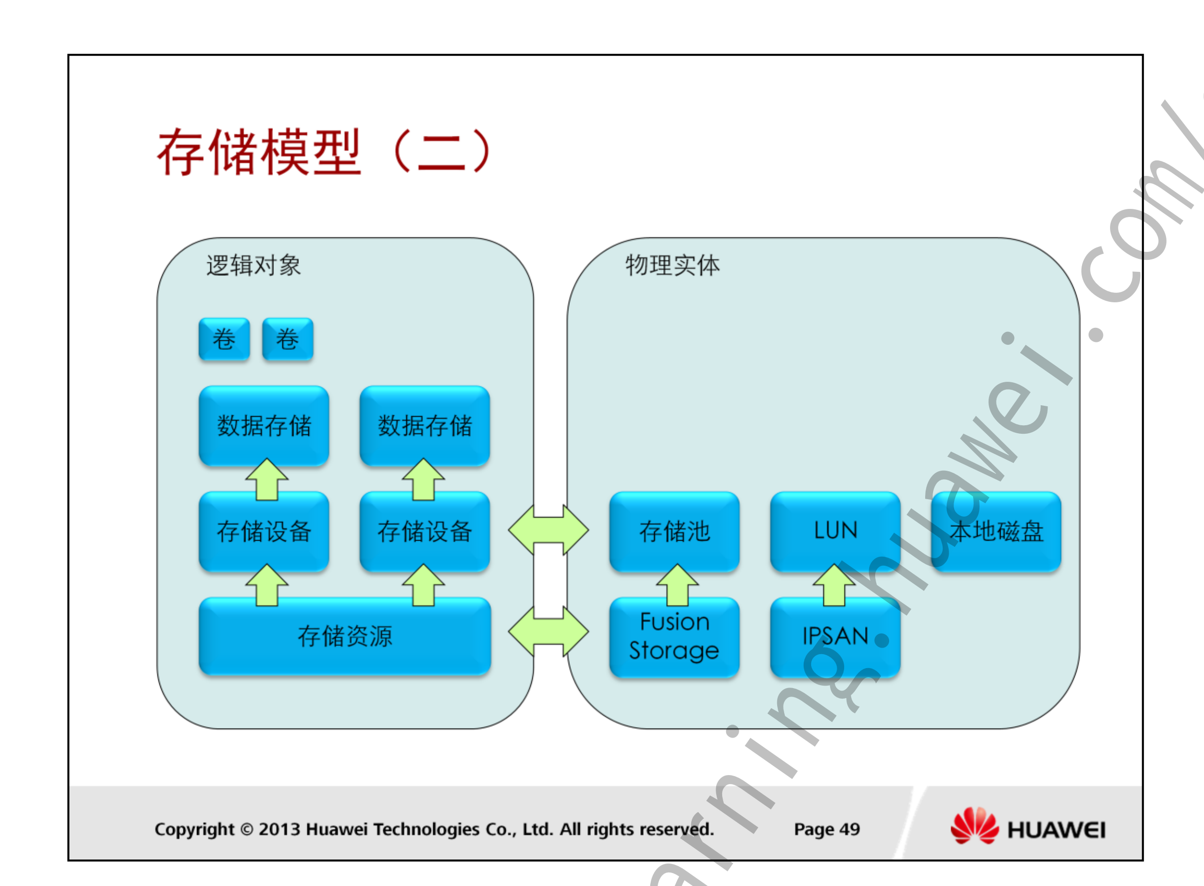
1. 云计算部署流程
2. 网络规划
3. 服务器规划
4. **存储规划**
5. FusionCompute部署
6. FusionManager部署
7. FusionAccess部署
8. 部署验证方法



存储模型（一）

- 存储资源
  - 存储资源表示物理存储设备，例如IPSAN、FusionStorage等
- 存储设备
  - 存储设备表示存储资源中的管理单元，类似LUN、 FusionStorage池等
  - 一个存储资源可以有多个存储设备
- 数据存储
  - 数据存储表示系统中可管理、操作的存储逻辑单元
  - 一个数据存储和一个存储设备对应
  - 数据存储承载了具体的虚拟机业务，例如创建磁盘等




存储模型（二）
逻辑对象
卷
卷
数据存储
数据存储
存储设备
存储设备
存储资源
物理实体
存储池
LUN
本地磁盘
Fusion Storage
IPSAN
Page 49
HUAWEI

存储资源

- 存储资源有两种，FusionStorage和IPSAN
  - FusionStorage是华为分布式共享存储，可以将各个CNA的本地磁盘利用起来，组成资源池，并按需提供存储单元给各个主机使用
  - IPSAN是通过iscsi链路和主机建立连接的，主机连接IPSAN后可以扫描存储设备（LUN）
- 主机访问存储资源：
  - 首先需要添加存储资源
  - 再选定主机并关联存储资源



存储设备

- 存储设备有两种，FusionStorage 资源池和LUN：
  - FusionStorage的存储资源有且仅有一个资源池
  - 通过IPSAN的管理软件可以配置LUN的数目和大小，一套IPSAN可以包含多个LUN
- 存储设备需要通过主机探测的方式进行扫描发现
  - 主机需要链接存储资源后才能扫描存储资源所包含的存储设备
  - 每个主机都能发现各自的存储设备，也能发现共享的存储设备



数据存储

- 数据存储是在存储设备上创建的逻辑管理单元：
  - 数据存储需要创建在指定的存储设备上，且一个存储设备只能创建一个数据存储
  - 数据存储和主机关联，为主机提供资源，数据存储可以关联到多个主机，一个主机也可以使用多个数据存储
- 数据存储的使用
  - 存储设备必须被添加为数据存储才能被使用
  - 数据存储可用于存放虚拟机磁盘、快照文件
  - 数据存储的大小依赖于存储设备的大小



创建存储资源

在存储管理页面中，添加存储资源





主机配置存储接口

在主机和集群页面中，选择配置页签中的系统接口页面，点击添加存储接口，进行存储接口的配置




主机关联存储资源

在主机和集群页面中，选择配置页签中的存储资源页面，可以将主机关联存储资源



查询主机WWN号

在主机和集群页面中，选择配置页签中的存储资源页面，可以查询到主机的启动器名称



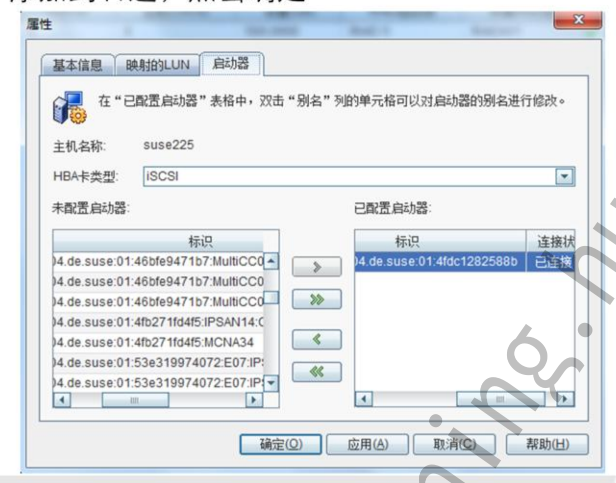

配置IPSAN（一）
登录到IPSAN管理页面，进行创建主机组、创建主机等操作
OceanStor ISM
系统(S) 配置(C) 告警(A) 用户(U) 安全(E) 帮助(H)
物理视图 逻辑视图
映射的LUN 主机
LUN名称
所有设备(1)
SN_2102315567Z09
未映射LUN
所有RAID组
RAID001
RAID002
所有主机组
默认主机组
Vmtest
修改主机组(M)...
删除主机组(D)...
创建主机(S)...
添加映射(A)...
删除映射(P)...
Page 57
HUAWEI


配置IPSAN（二）
在IPSAN管理页面，选定主机，点击右键配置主机启动器
物理视图
逻辑视图
映射的LUN
启动器
所有设备(1)
SN_2102315567Z09
未映射LUN
所有RAID组
RAID001
RAID002
所有主机组
默认主机组
Vmtest
Host001
Host002
LUN名称
修改主机(M)...
删除主机(D)
添加映射(A)...
删除映射(P)...
启动器管理(I)...



配置IPSAN（三）

在弹出的主机启动器页面中，左侧未配置启动中找到自己服务器的启动器名称，添加到右边，点击确定





HUAWEI

主机扫描存储设备

在主机和集群页面中，选择配置页签中的存储设备页面，可以扫描主机连接的存储设备





主机添加数据存储（一）

在主机和集群页面中，选择配置页签中的数据存储页面，可以将现有的存储设备添加为数据存储





主机添加数据存储（二）

添加数据存储过程中，需要选择相应的存储设备，并选择是否进行虚拟化。







目录



部署方案

节点类型	虚拟化部署	物理部署
VRM	虚拟化节点	物理节点
主机	物理节点	
ESC	虚拟化节点	物理节点
IMGS	虚拟化节点	物理节点

部署方案

节点类型	部署原则
VRM	支持单节点部署或主备部署，每个站点部署一个（单节点部署时）或一对（主备部署时）VRM节点
主机	根据客户对计算资源的需求部署多个主机，提供虚拟化计算资源。使用本地存储时，主机同时提供存储资源
ESC	ESC节点为可选管理节点。 支持单节点部署或主备部署。
IMGS	IMGS节点为可选管理节点，仅当部署ESC节点时，需要部署IMGS节点

部署原则



VRM：

支持单节点部署或主备部署，每个站点部署一个（单节点部署时）或一对（主备部署时）VRM节点。

虚拟化部署场景下，VRM节点部署在由管理集群的指定主机创建的虚拟机上。主备部署时需要将主备VRM节点分别部署在两台管理集群主机上。

物理部署场景下，VRM节点部署在物理服务器上。

主机：

根据客户对计算资源的需求部署多个主机，提供虚拟化计算资源。使用本地存储时，主机同时提供存储资源。

虚拟化部署场景下，需要指定主机创建VRM节点虚拟机。

为使每个集群内的计算资源利用率最优化，建议为同一集群下的主机配置相同的分布式交换机和数据存储。

ESC：

ESC节点为可选管理节点。

支持单节点部署或主备部署。

安装准备-PC要求

项目	要求
CPU	Intel或AMD X86架构的32位CPU
内存	2GB以上
硬盘	操作系统所在磁盘分区剩余空间大于1GB。 至少有一个非操作系统所在的磁盘分区剩余空间大于2GB。
操作系统	Windows XP/Windows 7 32位操作系统
系统软件	已安装JRE 1.6及以上版本。 已安装Microsoft .NET Framework 4.0及以上版本。 Windows XP操作系统需安装vcredist_x86。 Windows 7操作系统需按如下设置系统服务： • 在注册表中将“HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Control > Session Manager > Memory Management”目录中“LargeSystemCache”的值修改为“1”。 • 在注册表中将“HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > LanmanServer > Parameters”目录中“Size”的值修改为“3”。 • 单击“开始”，在“搜索程序和文件”中输入“services.msc”，按“Enter”，打开“服务”窗口重新启动名为“Server”的服务项。 说明：以Windows 7为例，选择“开始 > 控制面板 > 程序和功能”，在“卸载或更改程序”界面查看是否存在以下程序：“Java(TM) 6 Update *xx*”或“Java 7 Update *xx*”。 “Microsoft .NET Framework 4 Client Profile”及“Microsoft .NET Framework 4 Extended”。 如果软件未安装，需自行获取相应软件并完成安装。
网络	本地PC已与准备好的主机连接在同一台交换机，且IP地址设置为规划的管理平面空闲IP地址



- 安装FusionCompute时，需要一台本地PC，用于连接到主机网络进行安装。
- X86是复杂指令集（CISC）的代表，一般用于PC和服务器；而ARM则是精简指令集（RISC）的代表，一般用于手机。

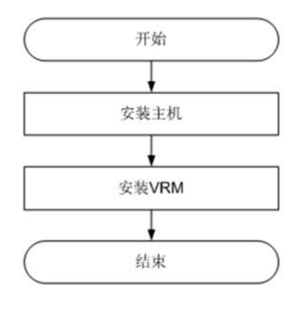
安装准备-下载软件包

软件包名称	软件名称	软件说明	获取方式
FusionCompute V100R003C00_Tools.zip	FusionCompute V100R003C00_InstallTool.zip	FusionCompute安装向导工具	**软件包下载路径：** “http://support.huawei.com/enterprise > 软件下载 > IT > 云计算 > 基础设施虚拟化 > FusionCompute > FusionCompute V100R003C00” **在软件包中的位置：** “installer\”
FusionCompute V100R003C00_CNA.iso	-	FusionCompute主机操作系统	**软件包下载路径：** “http://support.huawei.com/enterprise > 软件下载 > IT > 云计算 > 基础设施虚拟化 > FusionCompute > FusionCompute V100R003C00”
FusionCompute V100R003C00_VRM.zip	-	VRM虚拟机模板文件	



- 安装前要先下载软件包到本地PC。

安装流程



节点类型	虚拟化部署	物理部署
主机	虚拟化部署时，主机指所有物理服务器。 安装主机时需要为所有物理服务器安装操作系统，以提供硬件虚拟化服务。	物理部署时，主机指除VRM以外的所有物理服务器。 安装主机时需要为VRM以外的物理服务器安装操作系统，以提供硬件虚拟化服务。
VRM	安装在管理集群创建的虚拟机上。 虚拟机可使用服务器本地存储。	安装在物理服务器上。





安装主机

使用ISO安装包挂载到主机上，按向导安装主机操作系统和业务软件

- 浏览器输入http://待安装的主机BMC IP地址，登录BMC系统
- 打开远程控制窗口，为主机挂载镜像文件， 镜像文件名：FusionCompute V100R003C00_CNA.iso
- 重启主机
- 重启过程中，按“F11”，直到进入启动方式选择界面，选择从光盘启动
- 根据向导进行安装；安装过程中需配置主机IP、网关、密码等信息
- 完成主机安装，重启主机



安装VRM—选择安装模式

在本地PC上解压FusionCompute V100R003C00_Tools.zip，然后运行FusionCompute安装程序，开始VRM的安装





安装VRM—配置主机

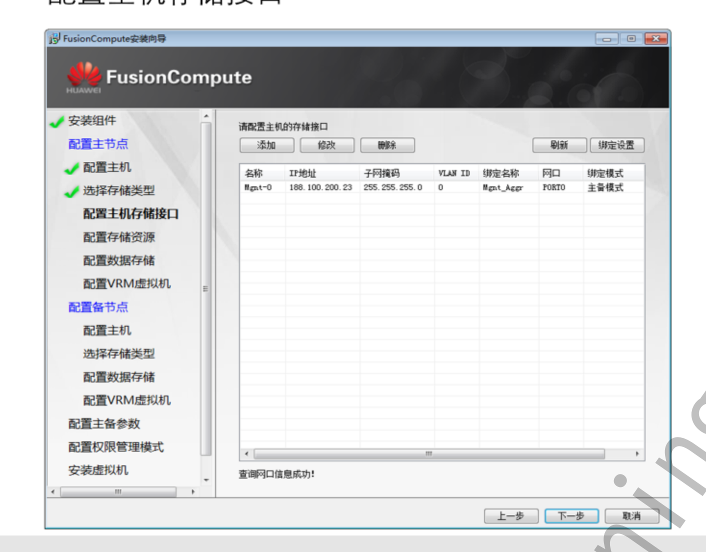
输入将安装VRM虚拟机所在的主机信息：IP地址、密码





安装VRM—配置主机存储接口

配置主机存储接口





安装VRM—配置存储资源

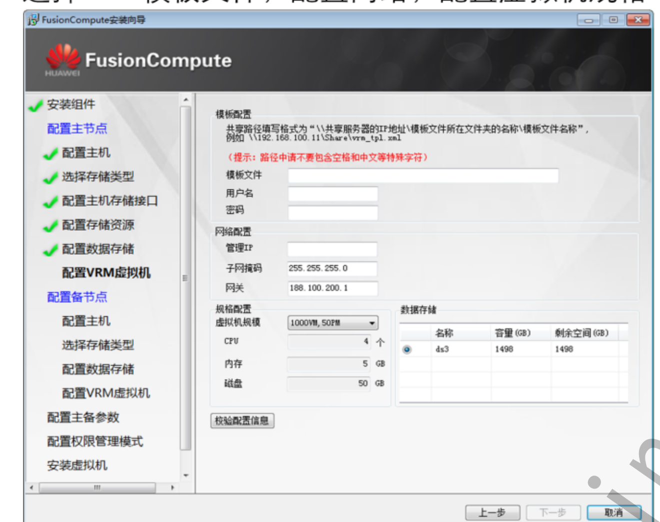
为主机添加和关联存储资源





安装VRM—配置VRM虚拟机

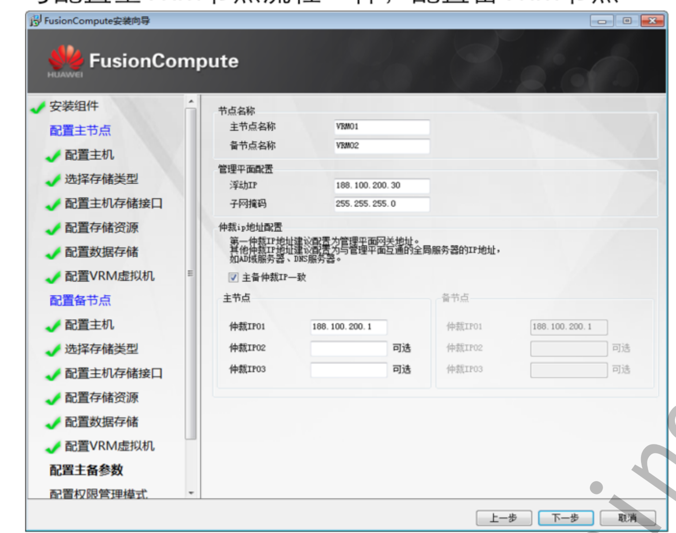
选择VRM模板文件，配置网络，配置虚拟机规格





安装VRM—配置备VRM节点

与配置主VRM节点流程一样，配置备VRM节点

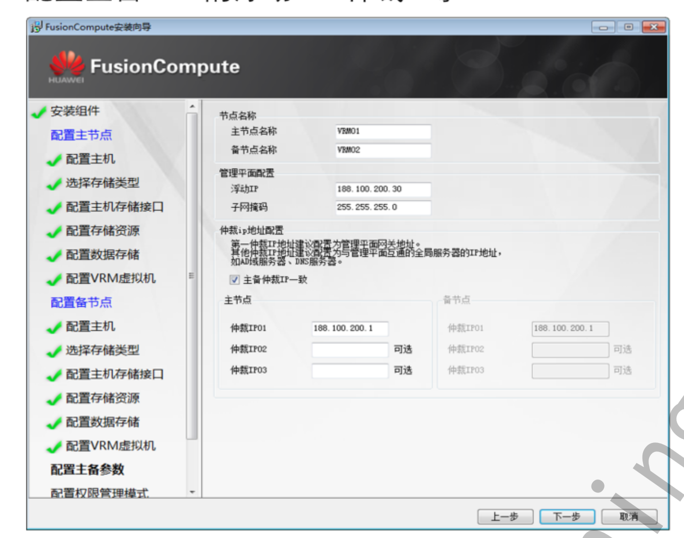




HUAWEI

安装VRM—配置主备参数

配置主备VRM的浮动IP、仲裁IP等





安装VRM—配置权限管理模式

两种权限管理模式

- 普通模式：拥有较高的易用性。在此模式下，单个帐户可以被授予系统内所有的操作权限。
- 高安全性模式：拥有较高的安全性。在此模式下，单个帐户只能拥有系统管理员、安全保密管理员和安全审计员三者中的一种身份。
  - 系统管理员仅能执行系统业务操作
  - 安全保密员仅能执行用户、角色的权限管理
  - 安全审计员仅能查看日志和告警信息，对其他用户的操作进行审查

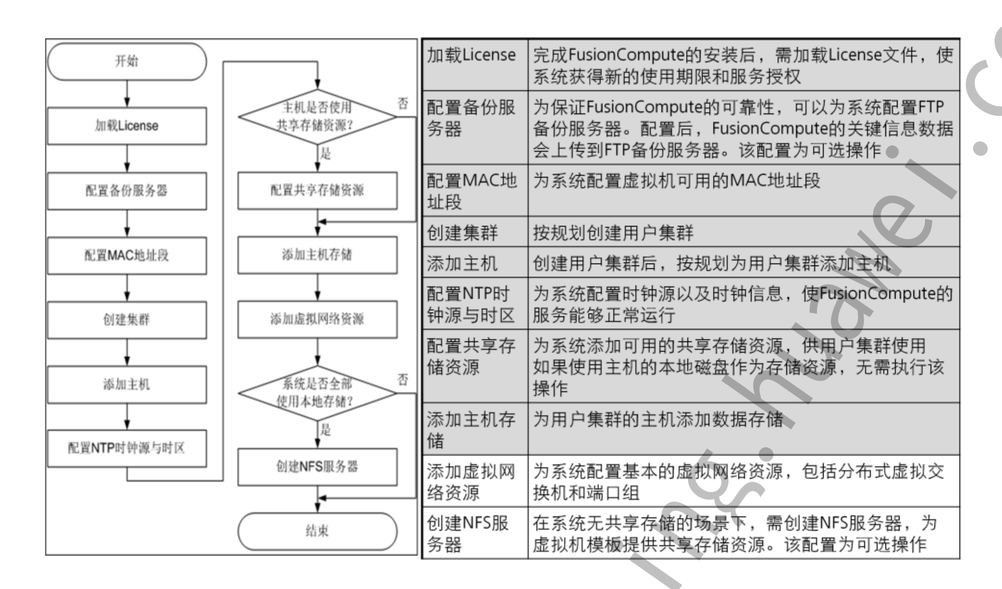


安装VRM—完成安装

- 配置完成后，系统开始创建VRM虚拟机，创建完VRM虚拟机后即完成整个FusionCompute软件的安装



配置流程



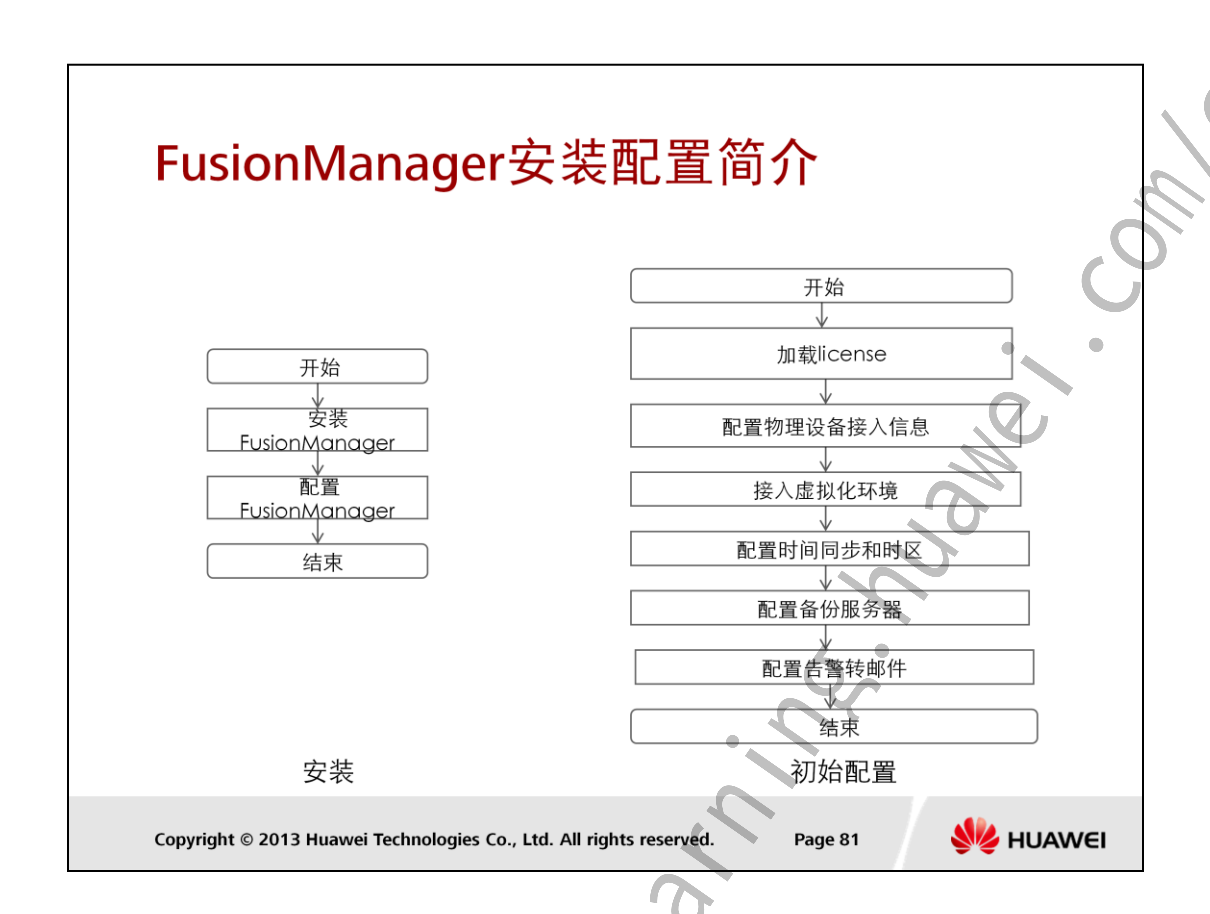
加载License	完成FusionCompute的安装后，需加载License文件，使系统获得新的使用期限和服务授权
配置备份服务器	为保证FusionCompute的可靠性，可以为系统配置FTP备份服务器。配置后，FusionCompute的关键信息数据会上传到FTP备份服务器。该配置为可选操作
配置MAC地址段	为系统配置虚拟机可用的MAC地址段
创建集群	按规划创建用户集群
添加主机	创建用户集群后，按规划为用户集群添加主机
配置NTP时钟源与时区	为系统配置时钟源以及时钟信息，使FusionCompute的服务能够正常运行
配置共享存储资源	为系统添加可用的共享存储资源，供用户集群使用 如果使用主机的本地磁盘作为存储资源，无需执行该操作
添加主机存储	为用户集群的主机添加数据存储
添加虚拟网络资源	为系统配置基本的虚拟网络资源，包括分布式虚拟交换机和端口组
创建NFS服务器	在系统无共享存储的场景下，需创建NFS服务器，为虚拟机模板提供共享存储资源。该配置为可选操作





目录





- 在FusionCube一体机场景下FusionManager已预安装好。

安装准备

- 本地PC要求

项目	要求
操作系统	安装32位Windows XP或Windows 7操作系统。操作系统语言为中文或英文
磁盘空间	确保其中一个磁盘的剩余空间大于30GB
应用软件	"Internet Explorer 8.0"及以上版本或者"Firefox 8.0"及以上版本的浏览器

- FusionManager所在虚拟机要求

项目	要求
操作系统	Novell SUSE Linux Enterprise Server11 SP1 64bit
内存	≥17000MB
CPU	≥1CPU
硬盘	≥280GB
网络要求	使用管理平面的分布式交换机和端口组
虚拟机蓝屏策略	不处理



安装准备

- 软件包

软件包	软件清单
FusionManager软件包	FusionManager V100R003C00_GMN_GS.iso FusionManager V100R003C00_GMN_GS.sha256

- 软件安装数据

项目	要求
管理IP地址	FusionManager的管理IP地址。 FusionManager主备部署时，分别准备主备节点的管理IP地址。
浮动IP地址	FusionManager的浮动IP地址。
管理平面网关IP地址	FusionManager的管理平面网关的IP地址。

- 初始配置数据
  - 数据中心数据
  - 资源分区数据
  - 虚拟化环境数据
  - 刀片服务器数据
  - 机架服务器数据
  - 存储设备数据
  - 交换机数据



软件安装

- 模板方式安装FusionManager
  - 当FusionManager虚拟化部署时，建议使用此方法安装，可以缩短安装时间
- ISO方式安装FusionManager
  - 在虚拟机上使用ISO镜像文件安装FusionManager
- 配置FusionManager
  - 配置管理IP地址，浮动IP地址和网关IP地址



- 模板方式安装FusionManager
  - 在FusionCompute中，选择“虚拟数据中心管理 > 虚拟机和模板”，导入FusionManager模板文件
- ISO方式安装FusionManager
  - 登录FusionCompute。
  - 选择“虚拟数据中心管理 > 虚拟机和模板”。进入“虚拟机和模板”页面。
  - 在“虚拟机”页签，在待部署FusionManager的虚拟机所在列，选择“操作 > 挂载光驱”。进入“挂载光驱”页面。
- 执行gmninit命令配置IP地址
- FusionManager支持主备双机的

ISO方式安装FusionManager（1/3）

- 挂载光驱
  - 登录FusionCompute，进入“虚拟数据中心管理 > 虚拟机和模板 > 虚拟机”页签，选择“操作 > 挂载光驱”。
  - 填写文件路径为“\\本地PC的IP地址\共享文件夹名称\镜像文件的名称”
  - 勾选“使用本机用户名和密码”，填写本地PC的用户名和密码
  - 勾选“立即重启虚拟机，安装操作系统”，单击“确定”



- 前提条件
  - 已完成FusionCompute的安装配置。
  - 已在FusionCompute上创建好符合安装要求的虚拟机。

ISO方式安装FusionManager（2/3）

- 安装操作系统
  - 单击“VNC登录”，进入虚拟机操作系统安装界面
  - 请在30秒时间内选择“Install”
  - FusionManager开始自动安装，耗时约1小时
  - 若FusionManager是主备部署，重复上述步骤安装备节点





ISO方式安装FusionManager（3/3）

- 卸载光驱
  - 在FusionCompute中，进入“虚拟数据中心管理 > 主机和集群 > 虚拟机”页签
  - 单击已安装操作系统的FusionManager虚拟机
  - 单击“卸载光驱”



初始配置

- 加载License
- 配置物理设备接入信息
  - 批量或单个导入数据中心、资源分区、主机、交换机及存储等硬件设备的信息，以实现对硬件设备的维护管理和监控
- 接入虚拟化环境
  - 将虚拟化环境接入到FusionManager系统中，以达到对虚拟化资源的管理
- 配置时间同步与时区
- 配置备份服务器
  - 配置第三方备份服务器，用于备份FusionManager的关键数据
- 配置告警转邮件



- 加载License
  - 在FusionManager中，选择“系统管理 > License管理”，上传License文件。
- 配置物理设备接入信息
  - 要配置的信息包括：数据中心，资源分区，刀片服务器，机架服务器，存储设备，交换机
  - 设备导入模板中的数据总数不能大于500条，模板文件需小于2MB，否则会引起导入失败。
- 接入虚拟化环境
  - 设置虚拟化环境的信息：名称、类型、版本、接入协议、IP地址、端口、用户名、密码、供应商、更新周期（小时）。
- 配置告警转邮件
- 置告警转邮件功能，以便通过邮件快速获取告警信息，及时、有效的维护系统
- 可以根据需求选择需发送邮件的告警级别。



目录





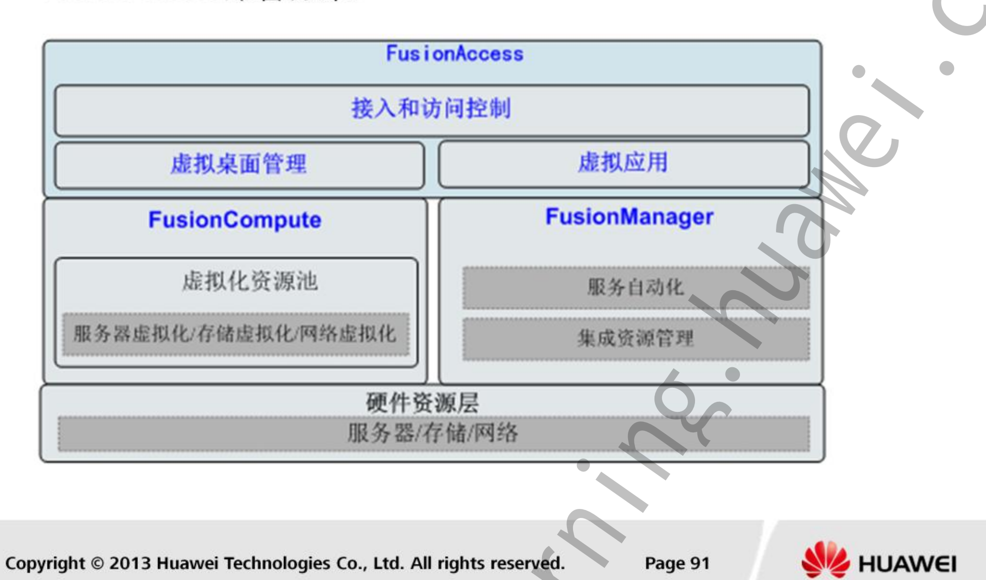
目录





解决方案位置

- FusionAccess部署方案：



软件结构

- FusionAccess包含的软件，如下图示：

用户Portal
FusionAccess
TCM
接入层
LB/AG
云终端
操作维护层
ITAC
LOG
虚拟桌面管理层
ITA
LS
DDC
WI
DB/Witness
虚拟应用层
XenApp
LS
WI
DB/Witness
现有IT系统
云平台

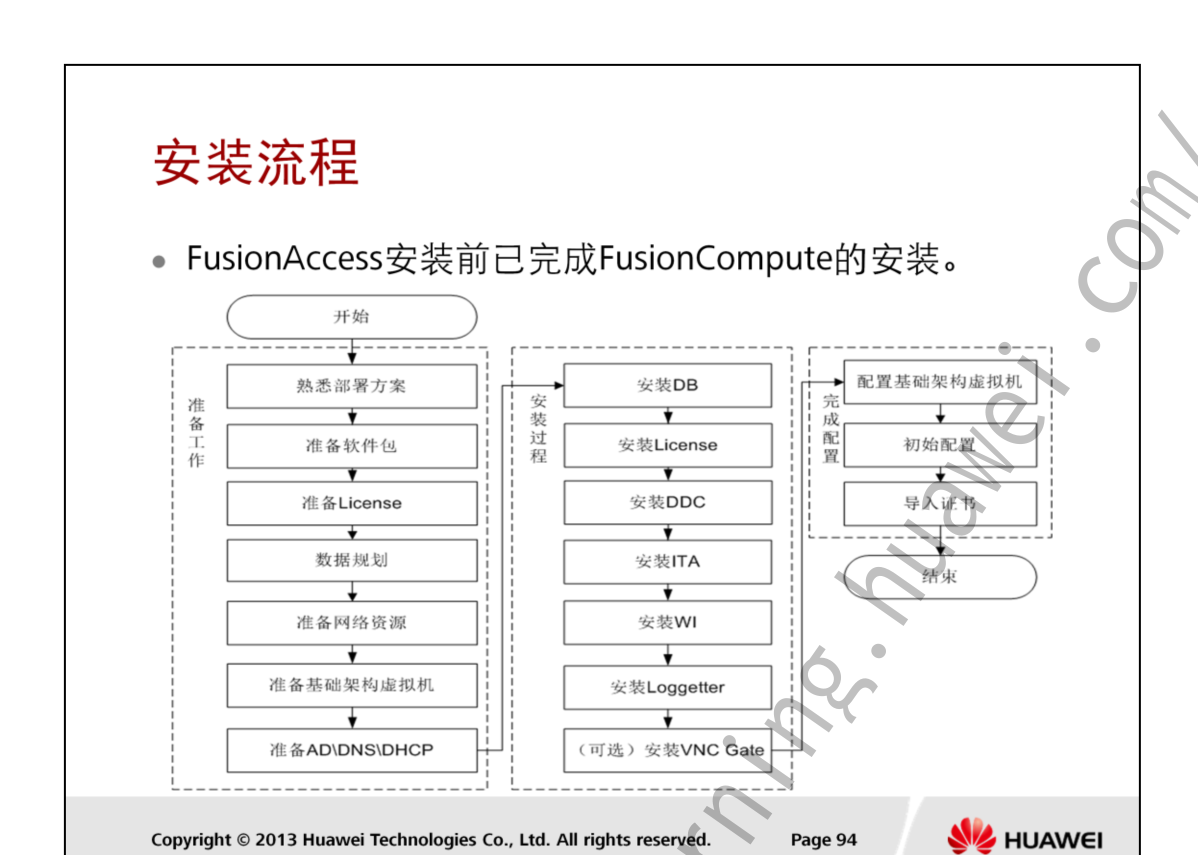
- AD：Active Directory
- DNS：Domain Name Server
- DHCP：Dynamic Host Configuration Protocol
- DDC：Desktop Delivery Controller
- ITA/ITAC：IT Adaptor
- WI：Web Interface
- DB：Database

部署方案

- FusionAccess推荐采用的标准部署方案：

部署组件	虚拟机规格	部署数量和部署方式
AD\DNS\DHCP	2VCPU/2GB内存/30GB系统盘/20GB用户盘/2块网卡	两台 基础架构域AD、DNS和DHCP组件合一部署： • 第一台VM：根域控制器、主用DNS、DHCP。 • 第二台VM：额外域控制器、备用DNS、DHCP。 为提高可靠性，建议两台VM部署在不同CNA（Computing Node Agent）节点上。
DB\WI\DDC\ITA	4VCPU/8GB内存/30GB系统盘/20GB用户盘/2块网卡	两台 两台VM必须部署在不同CNA节点上。
Loggetter\Witness\License\AntiVirus\Patch	2VCPU/2GB内存/30GB系统盘/30GB用户盘/2块网卡 **说明：** 如果TCM与“Loggetter\Witness\License\AntiVirus\Patch”服务器合一部署，虚拟机规格需要设置为“2VCPU/6GB内存/30GB系统盘/30GB用户盘/2块网卡”。	一台 Loggetter\Witness\License\Anti Virus\Patch组件合一部署。




安装流程
FusionAccess安装前已完成FusionCompute的安装。
开始
准备工作
熟悉部署方案
准备软件包
准备License
数据规划
准备网络资源
准备基础架构虚拟机
准备AD\DNS\DHCP
安装过程
安装DB
安装License
安装DDC
安装ITA
安装WI
安装Loggetter
（可选）安装VNC Gate
完成配置
配置基础架构虚拟机
初始配置
导入证书
结束
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 94
HUAWEI



目录



系统要求 - XenDesktop组件

- XenDesktop组件(WI/DDC/License)的要求，请参见：
  http://support.citrix.com/proddocs/topic/xendesktop-ibi/nl/zh/cn/cds-sys-reqs-wrapper-ibi.html?locale=cn
- ITA要求
  - 操作系统：Windows Server 2008 R2
  - 磁盘空间：215MB
- Loggetter要求
  - 操作系统：Windows Server 2008 R2
  - 磁盘空间：15MB
  - 收集日志和数据备份推荐的磁盘空间：25GB



- 软件安装时，PC机、存储设备、网关设备、网络环境等需要达到一定状态或者满足一定要求，才能保证FusionAccess正确安装。

系统要求 - PC、硬件

- FusionAccess软件安装和配置过程中，使用的PC机或便携机的要求：

项目	要求
操作系统	已安装Windows XP或Windows 7操作系统。操作系统语言为中文或英文。
硬盘空间	硬盘可用空间大于12GB，且单磁盘可用空间大于3GB。
应用软件	• 已安装Internet Explorer 8.0及以上版本或者Firefox 8.0及以上版本的浏览器。 • 已安装可解压.rar和.zip后缀的文件的解压缩软件，例如WinRAR。

- 安装FusionAccess时，对存储设备的要求：

类型	要求
IP SAN	一套基础架构系统，需要250GB存储空间。如果使用可选的增值特性引入的虚拟机或部署用户域，其所占用的存储空间另外计算。



系统要求 - 软件、网络

- 软件要求：
  - 安装FusionAccess时，需要完成FusionCompute软件安装。
- 安装FusionAccess时，对网络的要求：
  - 业务平面能正常互通。
  - 管理平面能正常互通。



准备软件包

软件类型	软件包名称	获取路径
操作系统安装文件	标准英文版Windows 2008 R2 SP1	下载路径：*待发布归档后更新此处。*
数据库及补丁文件	SQLServer 2008 R2	下载路径：*待发布归档后更新此处。*
	SQLServer2008R2 SP2补丁包	
	SQLServer 2008 R2 express	
XenDesktop软件	XenDesktop56.iso	下载路径：*待发布归档后更新此处。*
VDesktop软件	FusionAccess_Installer_V100R003C00.iso	下载路径：*待发布归档后更新此处。*
TC的SSL证书制作软件	TC&TCM Patch&Tools.zip	“http://support.huawei.com > 软件中心 > 版本软件 > 业务与软件 > 电信云计算 > CloudTerminal”
防病毒服务器端软件	TrendMicroAntivirus.zip	下载路径：*待发布归档后更新此处。*
补丁服务器软件	StandardComponents.zip	下载路径：*待发布归档后更新此处。*



- 请将所有需要的软件包直接下载到PC机的同一文件夹内。

准备License

- 使用华为提供的标准版Windows 2008 R2 SP1创建的虚拟机，其License只有30天试用期，必须购买正版的License文件并激活。
- FusionAccess的License申请周期通常需要3～5天，由华为技术支持工程师通过网站申请。



- 申请周期：通常需要3～5天。
- 申请方法：由华为技术支持工程师通过网站申请。
- 参考文档：《License 使用指南》（*待发布归档后更新此处*），请通过华为技术支持网站获取该文档。

数据规划

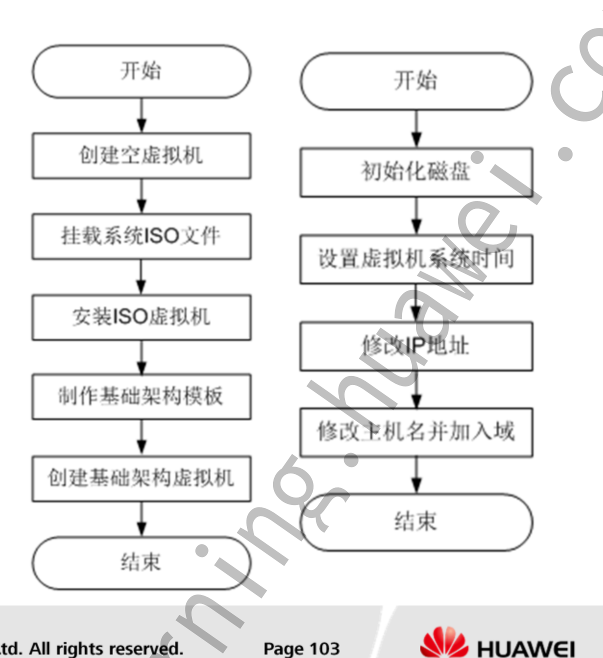
- 安装FusionAccess所需的基本数据
  - 准备网络资源数据
  - 创建基础架构虚拟机数据
  - 准备AD\DNS\DHCP数据、创建域帐号数据
  - 配置DDC服务器数据 、安装ITA服务器数据
- 对接局方AD所需的数据
  - AD\DNS\DHCP服务器IP、帐号、密码
  - 需要添加到客户的AD服务器白名单的虚拟机进程
- 安装防病毒和补丁服务器所需的数据



- 准备网络资源数据
  - 虚拟化平台:
    - FusionCube一体机虚拟化平台
      - 组网模式：二层模式、三层模式
        - 二层模式：VLAN池、外部网络、业务平面网关及掩码
        - 三层模式：子网、外部网络
    - 非FusionCube一体机虚拟化平台
      - VLAN池、外部网络、业务平面网关及掩码
- 创建基础架构虚拟机数据
  - 虚拟机名称:基础架构虚拟机名称。
  - 磁盘名称:基础架构虚拟机上挂载的用户磁盘名称。
  - IP地址:基础架构虚拟机业务平面和管理平面IP地址。
- 准备AD\DNS\DHCP数据
  - AD域名
  - AD服务还原模式密码
  - DNS反向解析IP地址段

准备基础架构虚拟机

- 创建基础架构虚拟机时，磁盘的配置模式推荐使用“普通”。
- 虚拟机创建完成后，需要配置虚拟机的相关信息。





准备AD\DNS\DHCP

- 需要准备AD\DNS\DHCP服务器来为FusionAccess桌面管理系统进行用户身份验证和管理、域名解析、IP地址分配等功能。
  - 准备AD\DNS\DHCP服务。
  - 准备域帐号：请根据各组件之间的合部情况，选择需要创建的域帐号。

域帐号	帐号说明	取值样例
DB\WI\DDC\ITA服务器	主、备服务器使用相同的登录域帐号。	dbuser
Loggetter\Witness\License\AntiVirus\Patch服务器	License服务器与日志、见证、防病毒服务器合一部署，使用同一帐号。	lsuser
域管理员帐号	用于域的管理。	vdsadmin
SQL服务域帐号	安装DB、设置DB镜像时用到的SQL服务帐号。	SQLServiceUser
Tomcat服务域帐号	ITA服务器中Tomcat服务启动帐号。 ▪ 新搭建的AD服务器，该帐号需要加入到基础架构域的管理员权限组里面，用于监控AD的告警。 ▪ 采用局方已有AD时，如果需要ITA监控局方AD的告警，则该帐号需要加入到局方AD的域管理员权限组里面。否则，无需加入到局方AD的域管理员权限组。	ITAServiceUser
备份服务域帐号	部署Loggetter服务器中用到的备份服务帐号。	LogServiceUser



- AD\DNS\DHCP属于IT基础组件，主要有以下两种部署场景：
  - 与客户的AD\DNS\DHCP对接：若局点已有AD\DNS\DHCP环境，并且规划FusionAccess组件与客户的AD\DNS\DHCP环境对接，则现场可以不用部署AD\DNS\DHCP服务器。
  - 新搭建AD\DNS\DHCP:对于局点需要部署AD\DNS\DHCP服务器的场景，具体操作可参见安装AD/DNS/DHCP。
- AD服务器部署完成后，需要登录AD服务器，创建各基础架构虚拟机登录和服务的域帐号。
  - 创建基础架构服务器OU:为便于域帐号管理，需要在AD服务器上创建基础架构服务器OU。
  - 创建域帐号:在基础架构OU中创建各基础架构虚拟机登录和服务的域帐号，需要创建的域帐号如图所示。
  - 创建域管理员：将上图中创建的域管理员帐号设置为基础架构域的管理员，即加入到“Domain Admins”组中。

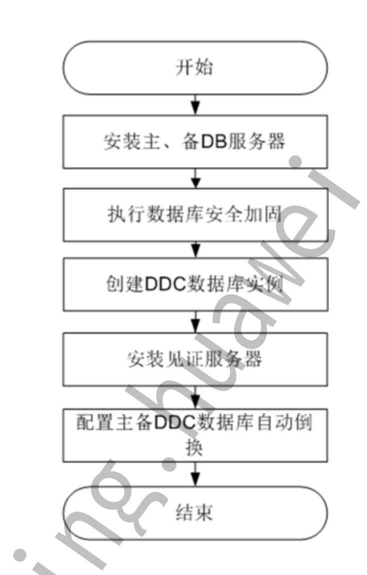


目录



安装数据库

- 前提条件：
  - 已完成基础架构虚拟机配置
- 准备数据：
  - SQL Server 2008 R2的Product Key
  - sa帐号密码
- 安装软件：
  - SQLServer2008R2.part1.rar
  - SQLServer2008R2.part2.rar

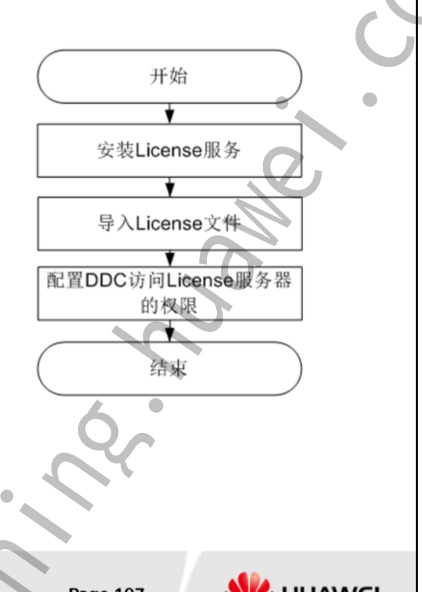




- 前提条件：已完成基础架构虚拟机配置，包括：
  - 设置IP地址。
  - 修改主机名并加入域。
  - 添加域帐号至管理员群组。
- 数据
  - SQL Server 2008 R2的Product Key
  - sa帐号密码
- 软件
  - 执行该任务需准备的软件如所示：

安装License

- 前提条件：
  - 已完成基础架构虚拟机配置
- 准备数据：
  - License服务器域管理员帐号和密码
- 准备软件：
  - XenDesktop56.iso

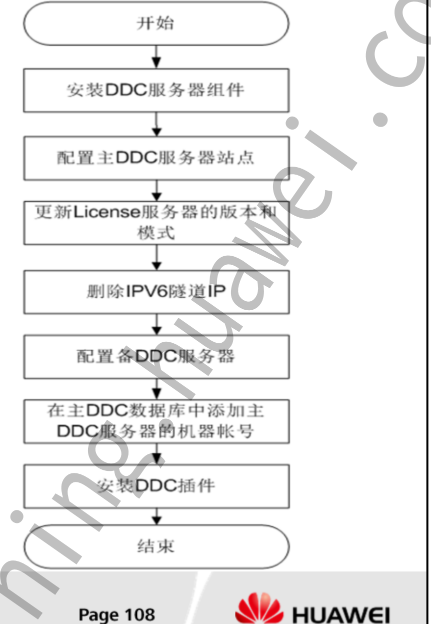




- 前提条件：已配置基础架构虚拟机IP地址、修改主机名并加入域。
- 准备数据：License服务器域管理员帐号和密码。
- 准备软件：XenDesktop56.iso，安装组件：License server

安装DDC

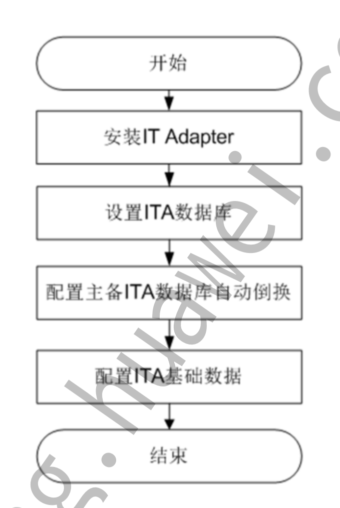
- 前提条件：已完成基础架构虚拟机配置、已完成DB、License的安装配置
- 准备数据：
  - DDC站点名 、数据库实例名、域管理员帐号和密码
  - ITA连接DDC数据库帐号
  - 主备DB服务器、见证服务器的数据库服务启动帐户（同一帐户）
- 准备软件：
  - XenDesktop56.iso
  - FusionAccess_Installer_V100R003C00.iso



- 前提条件:
  - 已完成基础架构虚拟机基本配置：设置IP地址 、修改主机名并加入域。
  - 已完成License服务器的配置：将DDC服务器域管理员帐号加入到License服务器管理员群组中。
  - 已完成DB服务器安装和配置
- 准备的数据：
  - DDC站点名
  - DDC数据库实例名
  - DDC服务器的域管理员帐号和密码。
  - ITA连接DDC数据库帐号
  - 主备DB服务器、见证服务器的数据库服务启动帐户（同一帐户）
- 准备的软件：
  - XenDesktop56.iso，安装组件：XenDesktop Controller 、Deskop Studio 、Desktop Director;若WI和DDC合一部署时，则需安装 “Web Access”组件。
  - FusionAccess_Installer_V100R003C00.iso

安装ITA

- 前提条件：已完成基础架构虚拟机配置、已完成DB、DDC安装配置
- 准备数据：
  - ITA连接数据库帐号
  - 主备DB服务器、见证服务器的数据库服务启动帐户（同一帐户）
- 准备软件：
  - FusionAccess_Installer_V100R003C00.iso





HUAWEI

- 前提条件：
  - 已完成部署ITA服务器的基础架构虚拟机配置。
  - 已准备DB服务器。
  - 已完成DDC服务器的配置。
  - 已在主DB服务器上创建ITA数据库。
- 数据
  - 执行该任务需要准备的数据将在步骤中介绍。
  - ITA连接数据库帐号
  - 主备DB服务器、见证服务器的数据库服务启动帐户（同一帐户）
- 软件
  - FusionAccess_Installer_V100R003C00.iso

安装WI

- 前提条件：
  - 已配置基础架构虚拟机。
  - 已安装DDC、ITA服务器
- 数据：无
- 软件
  - XenDesktop56.iso
  - FusionAccess_Installer_V100R003C00.iso

开始
配置操作系统文件
安装XenDesktop软件包中的WI组件
安装“WI PlugIn”
配置站点
结束

- 当WI和DDC合一部署时，如果在安装DDC时已经安装了“XenDesktop Controller”和“Web Access”组件，则无需执行“安装XenDesktop软件包中的WI组件”操作。
- 前提条件：
  - 已配置基础架构虚拟机。
  - 已安装DDC、ITA服务器。
- 数据：无
- 软件
  - XenDesktop56.iso
  - FusionAccess_Installer_V100R003C00.iso

安装Loggetter

- 前提条件：
  - 已完成基础架构虚拟机配置
- 准备数据：
  - FTP共享文件夹的路径
  - 日志服务的域帐号和密码
- 准备软件
  - FusionAccess_Installer_V100R003C00.iso
- 安装步骤：
  - 直接点击安装完成



- 前提条件：已完成基础架构虚拟机配置：
  - 设置IP地址
  - 修改主机名并加入域
- 准备数据：
  - FTP共享文件夹的路径
  - 日志服务的域帐号和密码
- 准备软件
  - FusionAccess_Installer_V100R003C00.iso

（可选）安装VNC Gate

- 前提条件：无
- 准备数据：
  - 网卡设置：第一块网卡为业务网卡，第二块为管理网卡。
  - 磁盘：系统盘大小为10G，无需用户盘。
- 准备软件
  - FusionAccess_VNCGate_template_V100R003C00.rar
- 安装步骤：
  - 直接点击安装完成





目录

7. **FusionAccess部署**



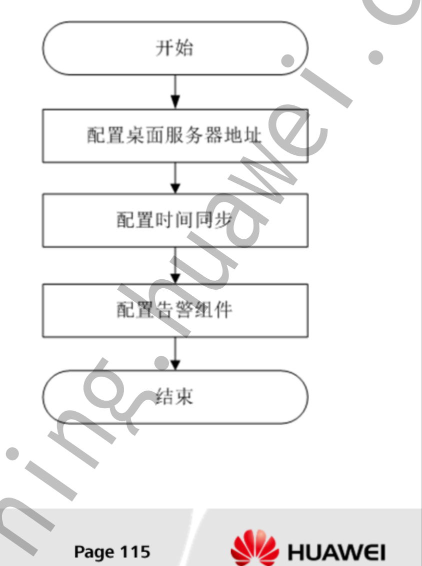
配置基础架构虚拟机

- 前提条件
  - 已创建各组件的基础架构虚拟机
  - 已安装AD/DNS/DHCP服务器，若用客户的AD且设置了白名单，则需把相关进程添加到客户AD的白名单中
- 准备数据：
  - Windows 2008 R2激活序列号
- 准备软件：
  - FusionAccess_Installer_V100R003C00.iso

- 前提条件
  - 已创建各组件的基础架构虚拟机。
  - 已安装AD、DNS和DHCP服务器，若使用客户的AD服务器，并且AD服务器设置了白名单，则需要把相关虚拟机进程添加到客户的AD服务器的白名单中。
- 准备数据：
  - 需要准备Windows 2008 R2的激活序列号。
- 准备软件：
  - FusionAccess_Installer_V100R003C00.iso

初始化配置

- 部署FusionAccess系统时，在完成各基础架构虚拟机安装配置后，需要进行桌面管理相关的初始配置
- 前提条件
  - 已获登录“FusionManager”的管理员帐号、密码。
- 准备数据
  - 主备ITA基础架构虚拟机的管理平面IP地址





HUAWEI

- 配置桌面服务器地址
  - 桌面服务器地址是指桌面业务管理系统对外提供服务的地址，系统根据此地址与桌面业务管理系统进行通信，必须配置。
- 配置时间同步
  - 配置AD服务器与上层时钟源同步，仅当用户将AD服务器部署在FusionAccess的基础架构虚拟机上时，需进行该配置。
- 配置告警组件
  - 该任务指导系统管理员，通过FusionAccess，配置各组件的IP地址信息，开启各组件的告警功能。

导入证书

- 前提条件：
  - 已安装WI服务器
  - 若Linux的TC，已将TC加入TCM
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址
  - 证书名称
  - 证书有效期

开始
是否使用Netscaler?
参加《Netscaler配置指南》
制作证书请求文件
创建CA服务器
制作证书
在WI上导入SSL证书
在终端上导入SSL根证书
结束

- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期



目录



验证部署流程

- 步骤一. 登录FusionCompute和FusionManager管理系统
- 步骤二. 检查系统状态及告警
- 步骤三. 健康检查工具
- 步骤四. 业务验证



- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期



- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期

登录FusionCompute管理系统检查

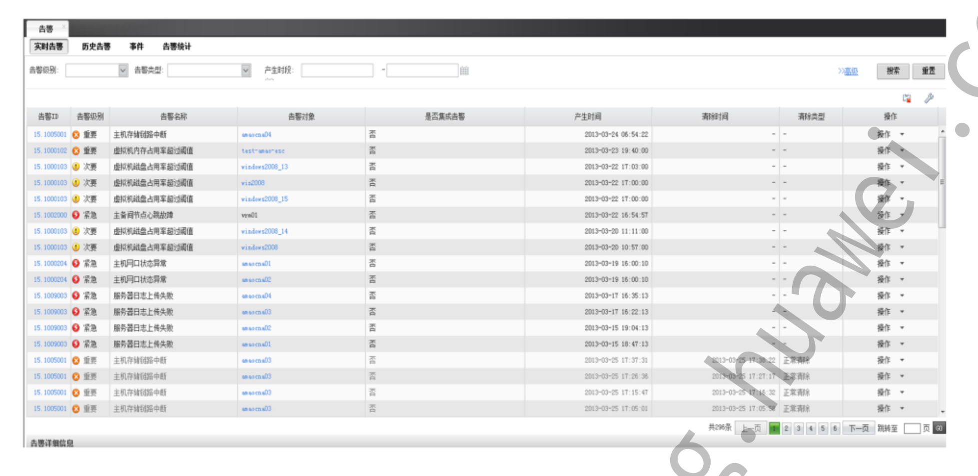


- 在主机和集群页面查看站点的概要页面，显示的信息是否正确



- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期

登录FusionCompute管理系统检查



- 检查FusionCompute的告警页面是否有部署相关的告警



- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期

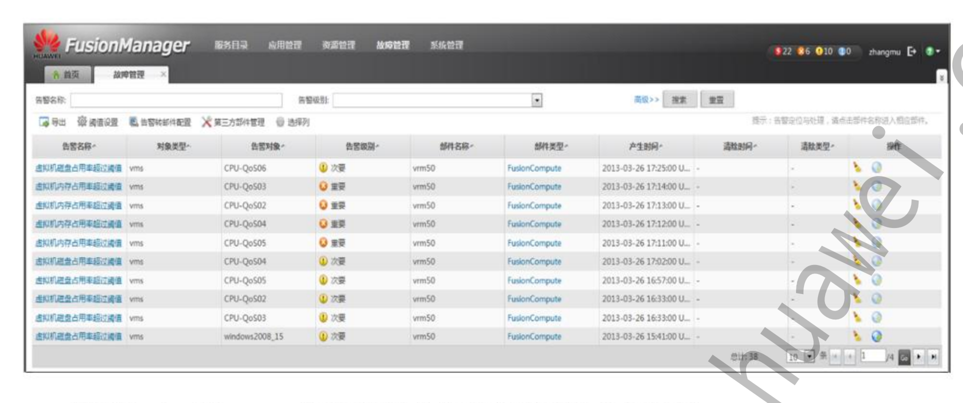
登录FusionManager管理系统检查



- 登录FusionManager，查看首页显示的信息是否与配置一致

- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期

登录FusionManager管理系统检查



- 检查FusionManager的告警页面是否有部署相关的告警



- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期

健康检查工具检查

- 执行健康检查工具
- 查看健康检查报告
- 无“不合格”检查项



- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期

业务验证

- 执行健康检查工具
- 查看健康检查报告
- 无“不合格”检查项



- 前提条件：
  - 已安装WI服务器。
  - 对于Linux操作系统的TC，已将TC加入TCM管理系统。
- 数据准备：
  - Common name
  - 证书服务器业务平面IP地址：证书服务器建议部署在AD服务器或WI服务器上。部署在AD服务器上，则为AD服务器的业务平面IP地址。 部署在WI服务器上，则为WI服务器的业务平面IP地址。
  - 证书名称
  - 证书有效期

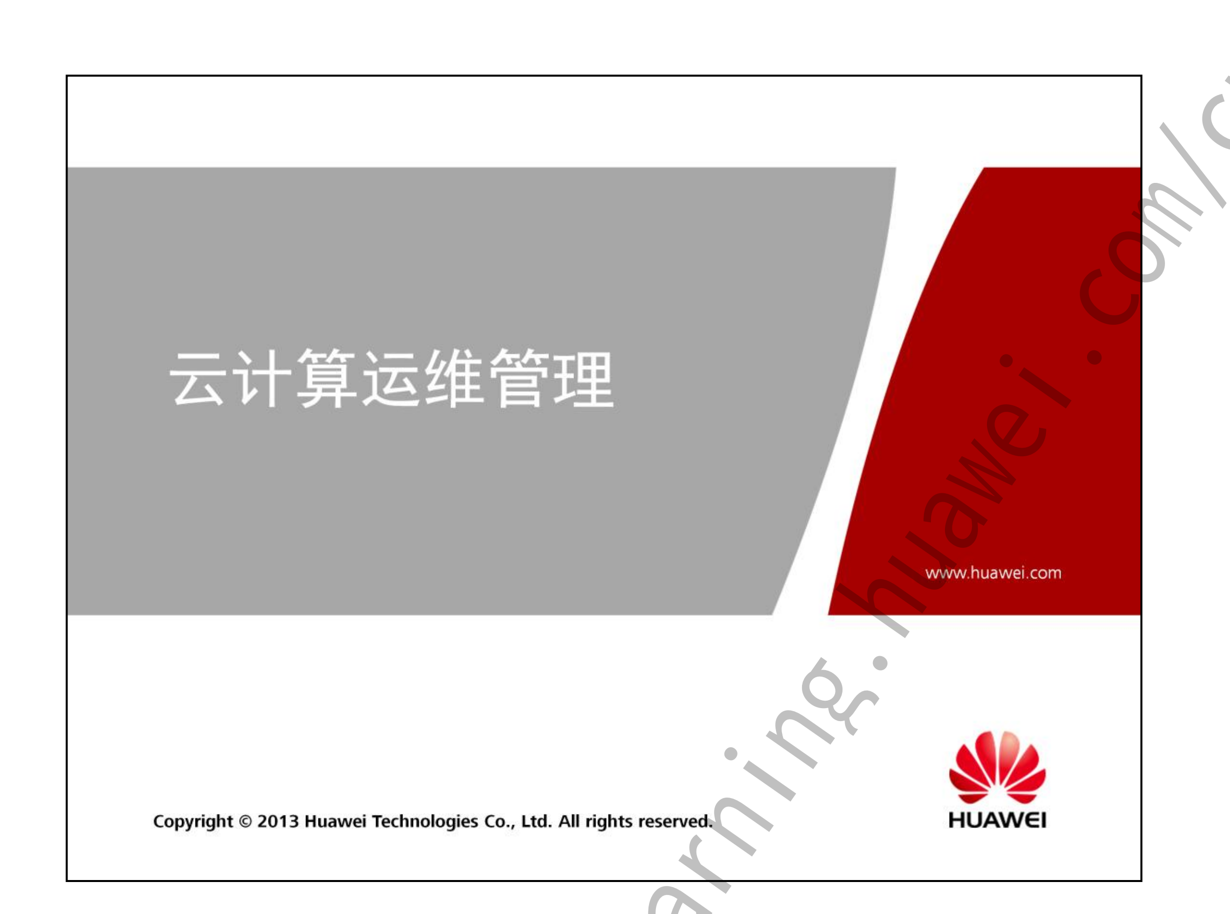


总结

- 云解决方案的安装部署流程
- 云解决方案硬件资源的部署
- 云解决方案软件系统的部署




Thank you
www.huawei.com


云计算运维管理
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录





运维管理系统

- 智能系统管理
  - 集中统一管理，提高维护效率；
  - 可视化，快速定位问题和恢复业务；

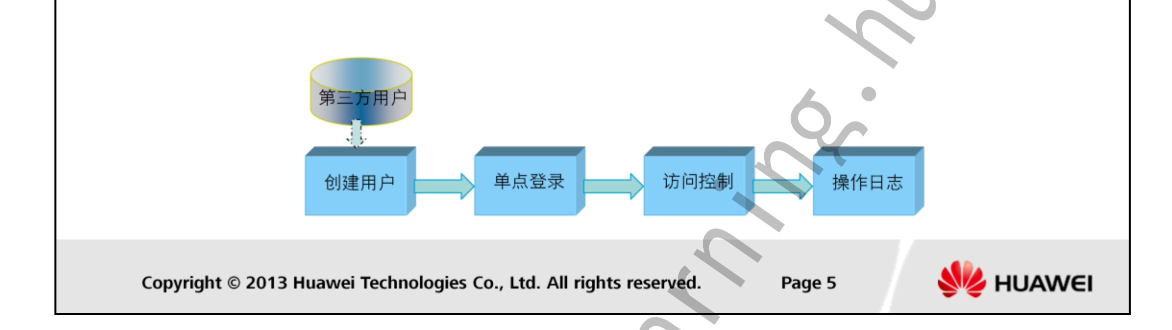


目录



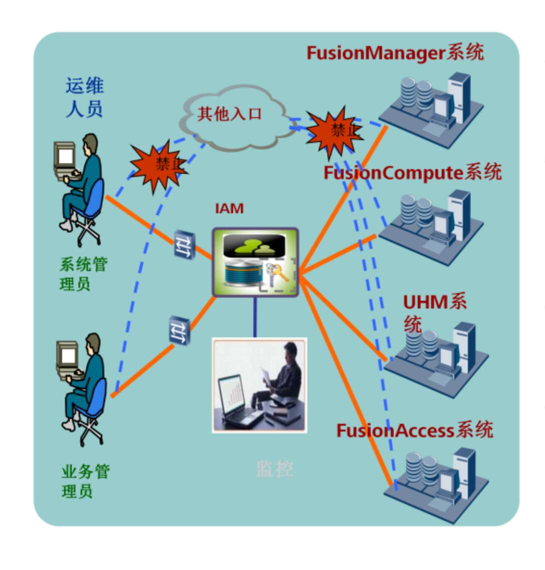
基于角色访问控制概念

- 基于角色访问控制
- 提供统一认证、统一授权、统一审计的功能
- 基于角色访问控制主要解决多点接入，分散管理，共享账号，访问控制不严，操作无法审计 的问题。



- 基于角色访问控制，基本思想：对于系统中的管理员，并 不是直接将权限赋给管理员，而是在管理员集合和权限集合之间引入角色集合，一旦管理员被分配适当的角色后，该管理员就拥有此角色的所有操作权限。
- 提供统一认证、统一授权、统一审计的功能，对一体机中的各个子系统提供统一的登录入口，对每个管理员提供统一的授权模式，对管理员在整个一体机的关键操作记录操作日志。
- 基于角色访问控制主要解决多点接入，分散管理，共享账号，访问控制不严，操作无法审计 的问题。

统一认证



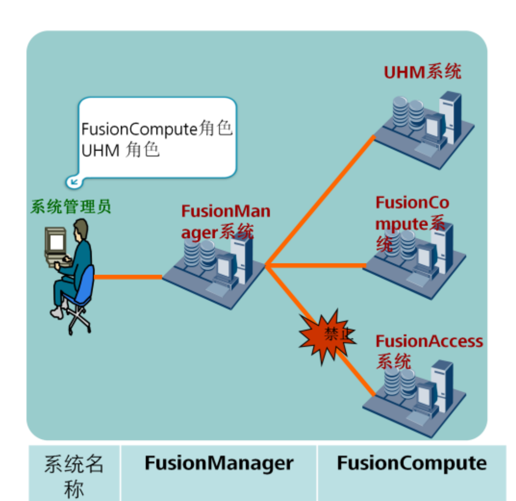
- 提供统一的访问入口，统一的认证机制
- 管理员在登入一个系统后，可以直接登入其他系统，不需要再次输入用户名、密码
- 管理员在一个系统退出后，其他系统也会自动退出。
- 具有会话超时机制，提高系统安全。

 Page 6



- 实现原理
- 管理员通过IAM登陆后，统一认证中心，会 给该管理员发放一个身份标识，表明该管理员已经认证通过。
- 管理员访问系统时，系统会获取管理员的身份 标识，验证管理员的合法性。

权限控制（1/2）

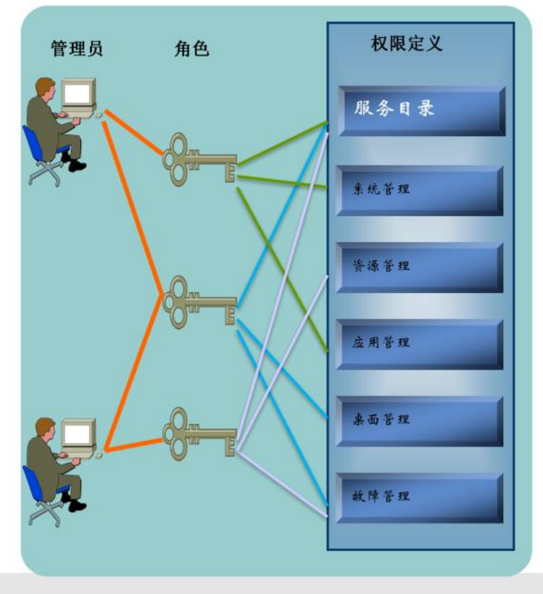


系统名称	FusionManager	FusionCompute
默认角色名称	系统超级管理员 系统操作员 系统查看员	系统超级管理员 系统查看员

- 每个管理员都具有FusionManager系统角色，该管理员也可以具有子系统的角色。
- 各个子系统提供默认角色。
- 可以给不同管理员赋予不同的角色，使管理员具有不同的职能。
- 管理员登入子系统时，子系统首先获取该管理员具有的角色信息，只有当管理员具有该系统角色时，才允许进入。
- FusionManager系统默认角色与子系统默认角色存在映射关系。



权限控制（2/2）



- 细粒度权限控制描述
- 管理员对核心业务的操作都进行鉴权控制。
- 可以根据业务的需要，将一组权限归属于一个角色，只有具有该角色的管理员，才能具有这些权限。
- 确保合法管理员对资源的控制，防止越权操作。



HUAWEI

- 鉴权原理
- GM系统中需要鉴权的操作都在IAM注册，权限定义区分业务管理员权限和系统管理员权限，IAM收集整个GM系统的权限信息。
- IAM对GM系统中的操作采用集中鉴权，所有的鉴权操作都在IAM完成。
- IAM同时存储VDI、UHM、GE子系统的默认角色，子系统查询用户角色时，将GM默认角色映射为子系统默认角色。
- 子系统利用管理员具有的角色，完成本地鉴权。

角色管理

- 创建角色
  - 默认角色：administrator，operator，auditor，resourcemanager
  - 角色类型：系统管理类角色和业务管理类角色
- 修改角色
- 删除角色
  - 有用户关联的角色不允许被删除



- 分为系统管理类角色和业务管理类角色，需要根据不同的权限选择用户类型。
- 业务管理类角色：可以具有创建服务目录、服务模板和应用管理的权限，还可以具有在首页查看资源使用状态及应用部署任务状态的权限。
- 系统管理类角色：可以具有所有子系统的操作权限



- 删除用户的操作有以下约束： 用户不能对自身进行删除。
- admin用户不能被删除。
- 要选择域domain和角色

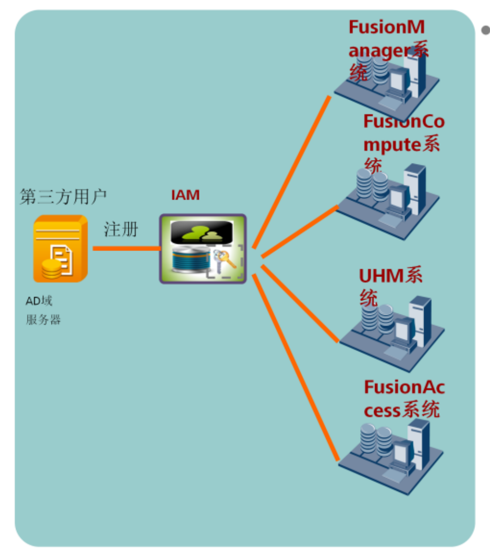
配置密码策略

- 配置了密码策略后，创建用户时设置的密码必须符合此密码策略
- 密码策略，如：
  - 密码最小字符数，密码有效期（天），用户锁定时长（分钟）等



- 设置如下参数，配置密码策略。
  - 密码最小字符数
  - 密码最大字符数
  - 密码是否必须包含特殊字符
  - 密码是否允许包含正序用户名或逆序用户名
  - 密码重复使用规则
  - 密码有效期（天）
  - 密码被重置和首次登录是否要求修改密码
  - 密码修改最短时间间隔（分钟）
  - 密码到期预先提醒时间（天）
  - 密码输入错误次数
  - 统计周期（分钟）
  - 用户锁定时长（分钟）

第三方AD对接



- 第三方对接描述
  - 目前IAM可以与采用AD域服务器的第三方IAM对接。
  - 第三方IAM的用户可以通过注册，作为FusionManager系统管理员或者FusionManager业务管理员，完成对一体机系统的运维。
  - 支持与AD域服务器的 SSL连接，提高安全性。

 Page 12



- AD:Active Directory
- IAM：Identifier and Access Manage，是FusionManager的一个模块
- 实现原理
  - AD认证用户通过注册，将用户的基本数据存放到IAM。
  - AD用户的认证数据仍然存放在AD与服务器，当AD认证用户登录时，IAM会到AD域服务器认证。



目录



性能监控

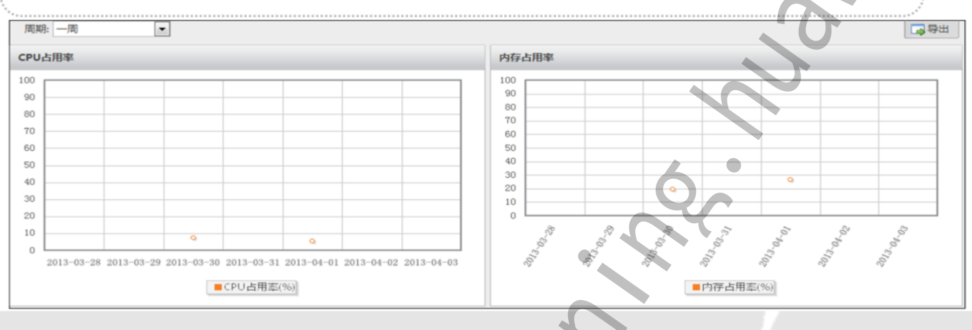
- 分析设备的各种指标数据，监控性能变化，防范性能风险， 分析单点负载情况，使用合理的均衡策略，保障业务畅通
  - 服务器监控
  - 交换机监控
  - 集群监控
  - 虚拟机监控

Page 14

HUAWEI

服务器性能监控

- 服务器性能指标：CPU，内存，网络和磁盘IO
- 实时性能监控
- 查询历史性能数据
  - 可以按周、月、年及自定义时段查询性能监控结果
  - 可以将性能报表文件保存到本地目录





- 在“监控信息”区域框中可查看以下主机信息。
  - CPU预留率
  - CPU预留容量
  - CPU可用容量
  - 内存预留率
  - 内存预留容量
  - 内存可用容量
  - CPU占用率
  - 内存占用率
  - 网络流入占用率
  - 网络流出占用率
  - 网络流出
  - 网络流入
  - 网络发送包速
  - 网络接收包速
  - 磁盘I/O写入
  - 磁盘I/O写出
  - 磁盘占用率

交换机性能监控

- 交换机实时性能指标：
  - 端口速率
  - 丢包率
  - 错误率

 Page 16 

- 在“端口连接状态”区域框中可查看交换机各端口的以下信息。
  - 端口编号
  - 状态
  - 发送速率
  - 接收速率
  - 发送丢包率
  - 发送错误率
  - 接收丢包率
  - 接收错误率

集群性能监控

- 集群性能指标：CPU，内存，网络
- 查询历史性能数据
  - 可以按周、月、年及自定义时段查询性能监控结果
  - 可以将性能报表文件保存到本地目录

周期：一周 导出

平均CPU占用率

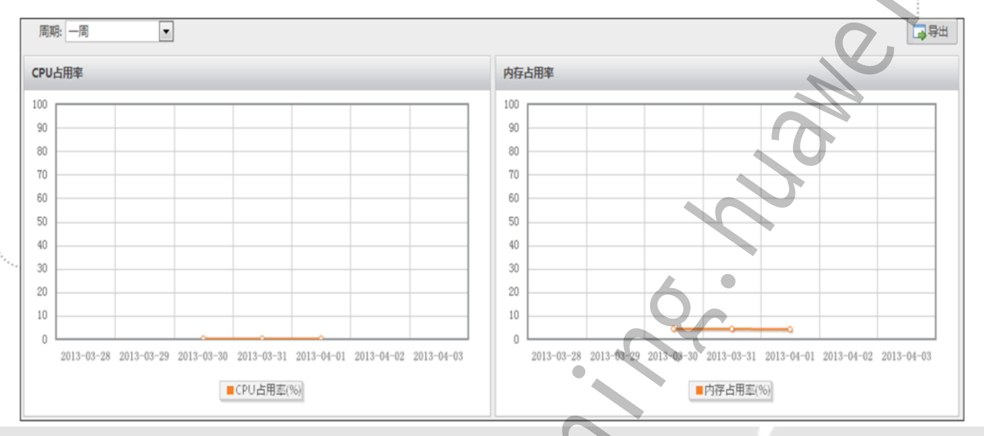
平均内存占用率

 Page 17 HUAWEI

- 在性能监控页面上通过以下图表查看集群的性能监控信息。
  - 平均CPU占用率
  - 平均内存占用率
  - 平均网络流速
  - TOP CPU占用主机
  - TOP 内存占用主机
  - TOP 存储占用主机
  - TOP 网络流入流速主机
  - TOP 网络流出流速主机

虚拟机性能监控

- 虚拟机性能指标：CPU，内存，网络和磁盘
- 实时性能监控
- 查询历史性能数据



 Page 18



- CPU占用率
- 内存占用率
- 网络流出
- 网络流入
- 磁盘I/O写入
- 磁盘I/O读出
- 磁盘占用率



目录

1. 运维管理概述
2. 权限管理
3. 系统监控
4. **告警管理**
5. 日志管理
6. 备份与恢复
7. TCM系统





- 支持按特定时间段、告警级别、告警对象、告警ID、告警名称和部件名称进行查询浏览

故障管理-告警灯和告警统计

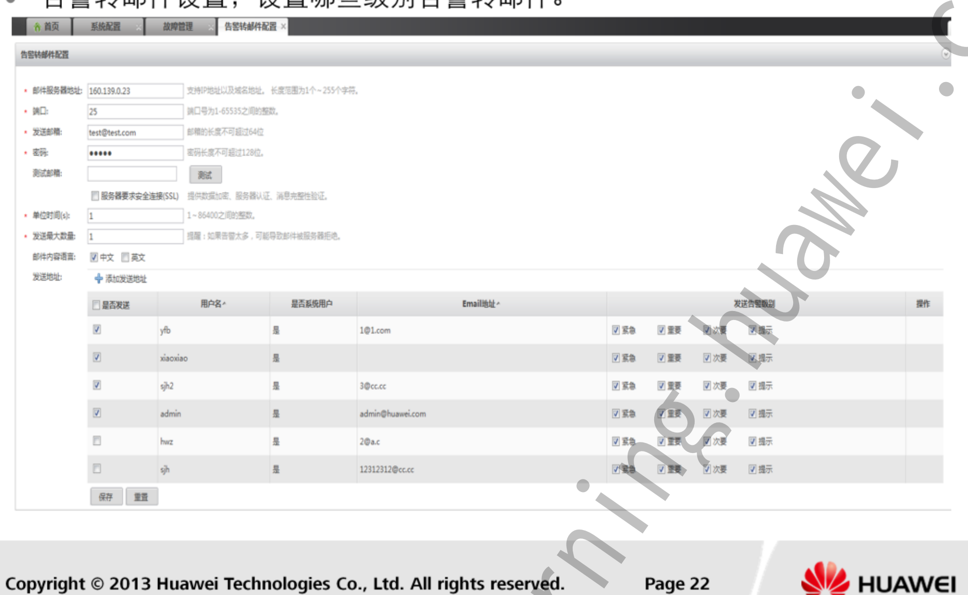
- 告警灯和告警统计：按告警级别紧急、重要、次要、提示来统计



HUAWEI

故障管理-告警转邮件

- 告警转邮件设置；设置哪些级别告警转邮件。



HUAWEI

故障管理-第三方部件管理

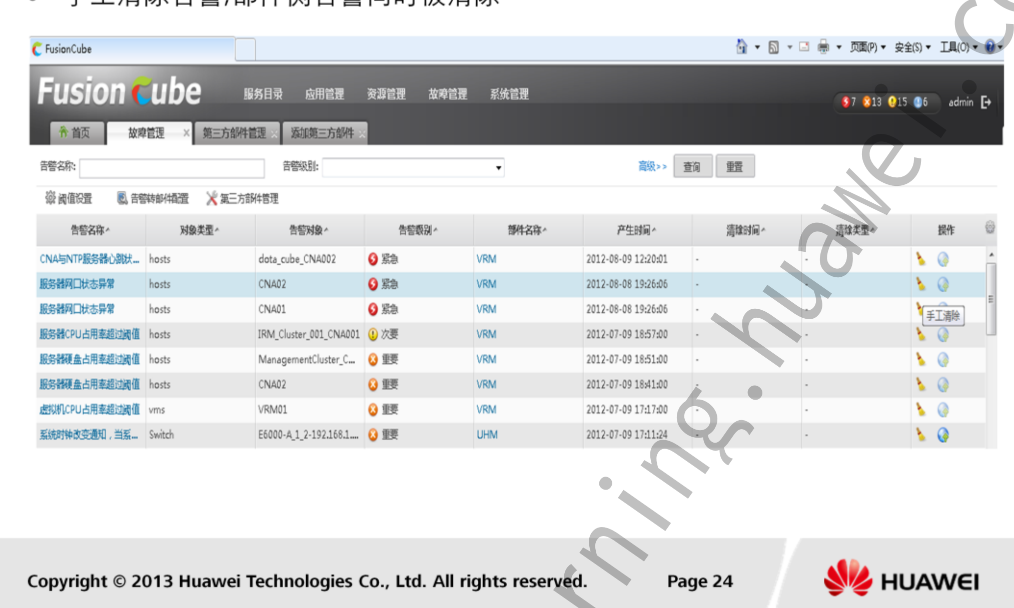
- 第三方部件管理，可以管理NetScaler和SVN部件告警
- SNMP trap接口



HUAWEI

故障管理-手工清除告警

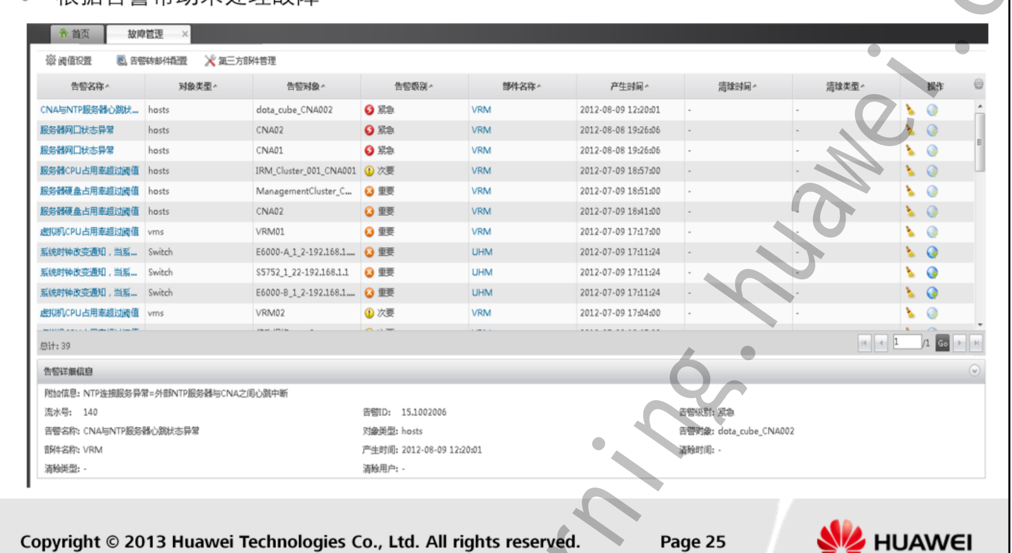
- 手工清除告警,部件侧告警同时被清除



HUAWEI

故障管理-查看告警详情

- 单击某条告警可以查看告警详细信息
- 根据告警帮助来处理故障



告警名称	对象类型	告警对象	告警级别	部件名称	产生时间	清除时间	清除类型	操作
CNA与NTP服务器心跳状...	hosts	dota_cube_CNA002	紧急	VRM	2012-08-09 12:20:01	-	-	
服务器网口状态异常	hosts	CNA02	紧急	VRM	2012-08-08 19:26:06	-	-	
服务器网口状态异常	hosts	CNA01	紧急	VRM	2012-08-08 19:26:06	-	-	
服务器CPU占用率超过阈值	hosts	IRM_Cluster_001_CNA001	次要	VRM	2012-07-09 18:57:00	-	-	
服务器硬盘占用率超过阈值	hosts	ManagementCluster_C...	重要	VRM	2012-07-09 18:51:00	-	-	
服务器硬盘占用率超过阈值	hosts	CNA02	重要	VRM	2012-07-09 18:41:00	-	-	
虚拟机CPU占用率超过阈值	vms	VRM01	重要	VRM	2012-07-09 17:17:00	-	-	
系统时钟改变通知，当系...	Switch	E6000-A_1_2-192.168.1....	重要	UHM	2012-07-09 17:11:24	-	-	
系统时钟改变通知，当系...	Switch	S5752_1_22-192.168.1.1	重要	UHM	2012-07-09 17:11:24	-	-	
系统时钟改变通知，当系...	Switch	E6000-B_1_2-192.168.1....	重要	UHM	2012-07-09 17:11:24	-	-	
虚拟机CPU占用率超过阈值	vms	VRM02	次要	VRM	2012-07-09 17:04:00	-	-	

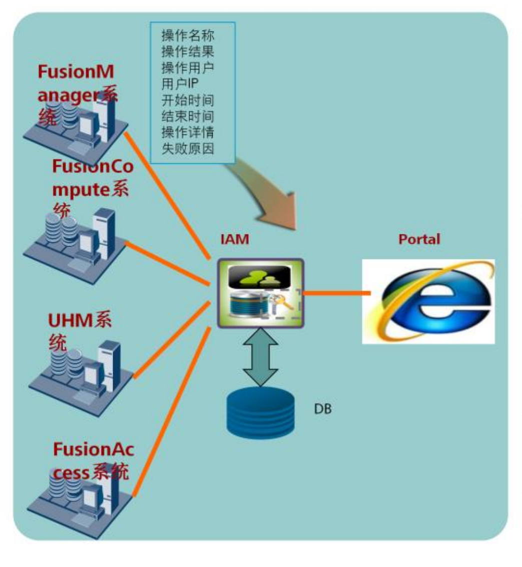
HUAWEI



目录



操作日志审计



- 对核心资源或者业务的操作记录操作日志，操作日志的内容包括操作名称，操作用户，用户IP，操作详情等信息。
- 提供操作日志导出功能，为用户对系统运行状况进行分析提供依据。
- 提供操作日志过滤查询的功能。
- 对管理员在系统上的操作记录实现事后追踪。
- 四种级别：高危 危险 一般 提示



- 操作日志审计原理
- 各个子系统将操作日志记录到IAM，IAM存储到数据库，最终呈现给用户。
- 按照用户输入的查询条件，对操作日志进行过滤，只呈现用户希望看到的操作日志。

定位信息收集-运行日志

- 系统运行日志收集
  - FusionManager运行日志
  - UHM运行日志
  - 主备VRM运行日志
  - CNA运行日志

```
[2013-02-27 17:02:35,610 +0800] [ERROR] [pool-2-thread-30] [com.galaxmanager.irm.connector.common.ConnectorLoginThread 244]
ConnectorLoginThread proxy login failed getConnector is Connector [id=1, name=null, urn=null, ip=160.148.0.171, activeIp=null,
standbyIp=null, port=8088, userName=GMRest, authToken=null, protocol=null, type=Uhm, isAvailable=false, isLogining=true,
language=zh_CN, domain=null, description=null]!
```




- 系统运行日志收集
- GalaxManager运行日志：
- /var/log/GalaxManager
- 2、UHM运行日志：
- /opt/UHM/Runtime/LegoRuntime/logs
- /opt/UHM/Runtime/Tomcat6/logs
- 3、主备VRM运行日志
- 当前日志：/var/locallog
- 转存日志：/var/backuplog/galaxenginelog/
- 4、CNA日志
- 当前日志：在各个CNA节点/var/log/galaxenginelog/路径下。
- 每15分钟上传日志在GalaxManager服务器的/opt/cnalog路径下。



目录



自动备份

- FusionManager、UHM、FusionCompute每天凌晨02:00自动进行备份。默认最多保留7个备份（包括自动和手工备份）。
- 备份存放路径
  - FusionManger：/opt/gmbackup/db/gmdb-[YYYY]-[MM]-[DD]-[sn].dump
  - UHM：/opt/UHM/Runtime/LegoRuntime/uhm/system/mysql/UHM_[sn].zip
  - FusionCompute：
    - 数据库备份文件：/var/backup/[YYYY]-[MM]-[DD]_sn/DATA
    - 配置备份文件：/var/backup/[YYYY]-[MM]-[DD]_sn/DB

 Page 30



- 备份的目的：系统数据丢失或破坏后，通过备份的数据把系统恢复过来。

FusionManager 手工备份

- 本地备份
  - 使用“PuTTY”工具，登录FusionManager。
  - 执行命令：backupGalaxManager -U cloudmgr -h localhost -p 2345
  - 到以下路径查看备份文件：/opt/gmbackup/db/manualbk/
- 备份FusionManager数据到第三方备份服务器
  - 使用“PuTTY”工具，登录FusionManager。
  - 执行命令：

    remoteBackupMgr -e -U [ftps用户名] -P [ftps密码] -h [ftps的IP地址] -p [ftps端口号]
  - 登录到第三方备份服务器查看备份文件。

Page 31



FusionManager 数据手工恢复

- 在对FusionManager进行重大操作（如升级或打补丁、重大数据调整、扩容等）后，系统有可能出现异常或未达到预期结果。此时需要对其进行回退，回退过程中需要进行数据恢复操作。
  - 使用WinSCP将第三方备份服务器的备份数据上传到FusionManager。
  - 使用“PuTTY”工具，登录FusionManager。
  - 执行命令：restoreGalaxManager -U cloudmgr -h localhost -p 2345 -f [备份文件全路径]
  - 登录FusionCube界面验证恢复结果。
- 注：恢复过程中会把FusionManager的进程停掉。



UHM手工备份

- 本地备份
  - 使用“PuTTY”工具，登录UHM。
  - 执行命令：

    cd /opt/UHM/Runtime/LegoRuntime

    sh ./uhm/system/mysqlbackup.sh [*数据库密码***] [***文件保留份数***]**
  - 到以下路径查看备份文件：/opt/UHM/Runtime/LegoRuntime/uhm/system/mysql
- 备份UHM数据到第三方备份服务器

Page 33



- 注：数据库默认密码为CloudStor@123

UHM 数据手工恢复

- 在对UHM进行重大操作（如升级或打补丁、重大数据调整、扩容等）后，系统有可能出现异常或未达到预期结果。此时需要对其进行回退，回退过程中需要进行数据恢复操作。
  - 使用WinSCP将第三方备份服务器的备份数据上传到UHM。
  - 使用 “PuTTY”工具，登录UHM。
  - 停止UHM服务：

    ```
    cd /opt/UHM/Runtime/bin
    sh shutdownSystem.sh
    ```

  - 执行恢复命令

    ```
    cd /opt/UHM/Runtime/LegoRuntime/uhm/system/mysql
    sh ../mysqlrestore.sh [数据库密码] [备份文件名]
    ```

  - 启动UHM服务

    ```
    cd /opt/UHM/Runtime/bin
    sh startSystem.sh
    ```

  - 登录系统界面验证恢复结果。

Page 34
HUAWEI



- 注：恢复过程中需要把UHM的进程停掉。



FusionCompute手工备份

- 使用 “PuTTY”工具，登录FusionCompute。
- 执行命令：cronBackupUpload
- 到路径/var/backup/[YYYY]-[MM]-[DD]_[sn]查看备份文件：
  - DATA目录下存放数据库备份文件。
  - DB目录下存放配置备份文件。

Page 35



- 注：如果要将备份VRM数据到第三方备份服务器，在执行cronBackupUpload前执行下面命令配置第三方备份服务器信息。
- setConfig

FusionCompute数据手工恢复

- 以下操作以恢复主用VRM节点的数据为例。
- 使用WinSCP将第三方备份服务器的备份数据上传到VRM。
- 使用“PuTTY”工具，登录主VRM。
- 停止VRM服务 service watchdog stop
- 执行恢复命令主VRM数据
  - restoreGeData -t DATA -f /home/DATA/ [备份文件名]
  - restoreGeData -t DB -f /home/DB/[备份文件名]
- 安全重启主VRM节点 reboot
- 登录系统界面验证恢复结果。

 Page 36



- 注：恢复过程中需要把VRM的服务停掉。

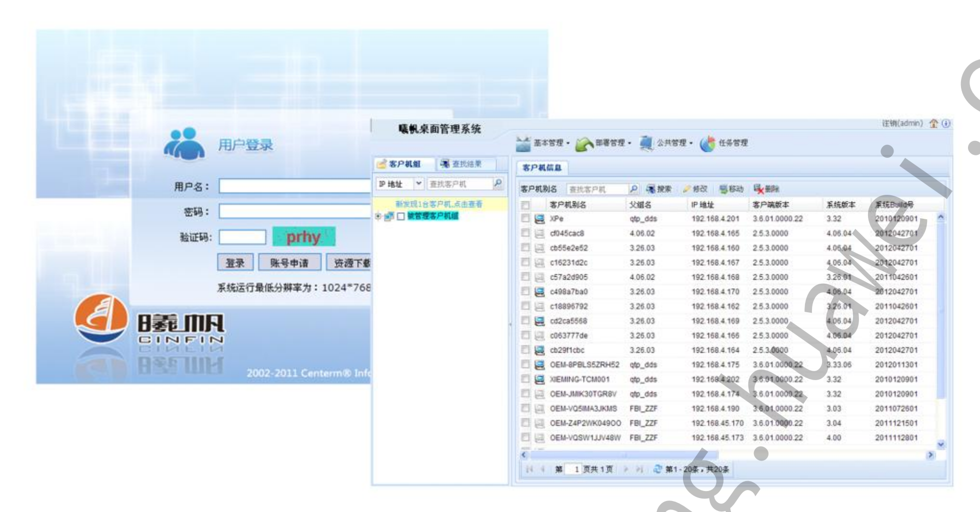


目录

1. 运维管理概述
2. 权限管理
3. 系统监控
4. 告警管理
5. 日志管理
6. 备份与恢复
7. **TCM系统**



TCM－TC终端管理系统



TCM终端管理系统是一套基于Browser/Server 的桌面管理系统。支持华为公司出品的CT系列Xpe、Linux 客户机的远程管理操作。



TCM的功能概述

TCM
三大功能模块

基本管理：该模块是进行主要的客户机管理操作的模块，支持客户机的桌面配置、远程协助、电源控制等功能。

部署管理：实现对客户机的文件复制和安装。

公共管理：通用的模块，包括对管理员权限的管理、管理员的操作日志和客户端的升级。

 Page 39



TCM-基本管理

功能项			描述
基本管理	系统配置	客户机参数配置	系统配置是对客户机操作系统及应用软件的参数信息进行配置，常见的系统配置包括显示、时间日期、系统用户、网络、浏览器、打印机、连接条目及其它应用软件的参数配置。
		模版管理	系统配置种的模版管理模块可以实现对批量的客户机设备进行参数配置。
		时间同步	设定Linux和Xpe机器的时间同步参数。
	远程协助		针对Linux自由版和Xpe的远程协助
	电源管理		进行开关机操作等
	消息管理		管理员与客户机用户的消息记录，管理员与客户机用户沟通的重要平台。
	性能监控	性能报警统计	性能监控是对计算机性能的动态概述。通过对客户机各项性能进行监控，方便跟踪客户机的运行状态，对突发状况进行及时的处理。同时，通过报表的分析统计，使用户对客户机的性能有全局的了解。
		实时性能监控	
		性能报警管理	

 Page 40 HUAWEI

- 基本管理：该模块是进行主要的客户机管理操作的模块，支持客户机的桌面配置、远程协助、电源控制等功能。

TCM-部署管理

功能项		描述
部署管理	Linux文件部署	针对Linux机器的系统升级、补丁升级和Agent升级。
	Windows文件部署	针对Xpe客户机的软件分发和复制文件。
	Windows系统镜像	针对Xpe的系统镜像抓取和系统镜像分发。
	资源中心	管理存储节点

HUAWEI

- 文件部署主要用于对系统中的文件进行部署，包括文件的复制和软件的分发，主要适用于对客户机应用软件的批量安装，文件的批量下发等。同时，通过文件部署，还可以对系统中的文件进行管理，包括文件的上传和删除等。

TCM-公共管理

功能项			描述
公共管理	客户机升级		实现Xpe版本的客户端Agent升级功能。
	用户管理	基本用户管理	用户管理用于帮助企业建立系统运行的账户信息，包括：管理员组划分、新建/修改管理帐户、角色管理、账户权限分配、帐号申请/审核等功能。管理员的权限根据角色来划分，帐号申请/审核方便大型企业快速地建立系统运行的账户信息。
		帐号审批	
		角色管理	
	电子标签		实现对客户机的维保时间管理。
	日志管理	日志操作管理	管理各种操作记录，记录管理员的操作时间、操作内容、操作结果，通过查询可以知道过去对系统操作的情况，方便日后事件跟踪。
		日志备份管理	
	其它管理	全局参数设置	设置全局的参数





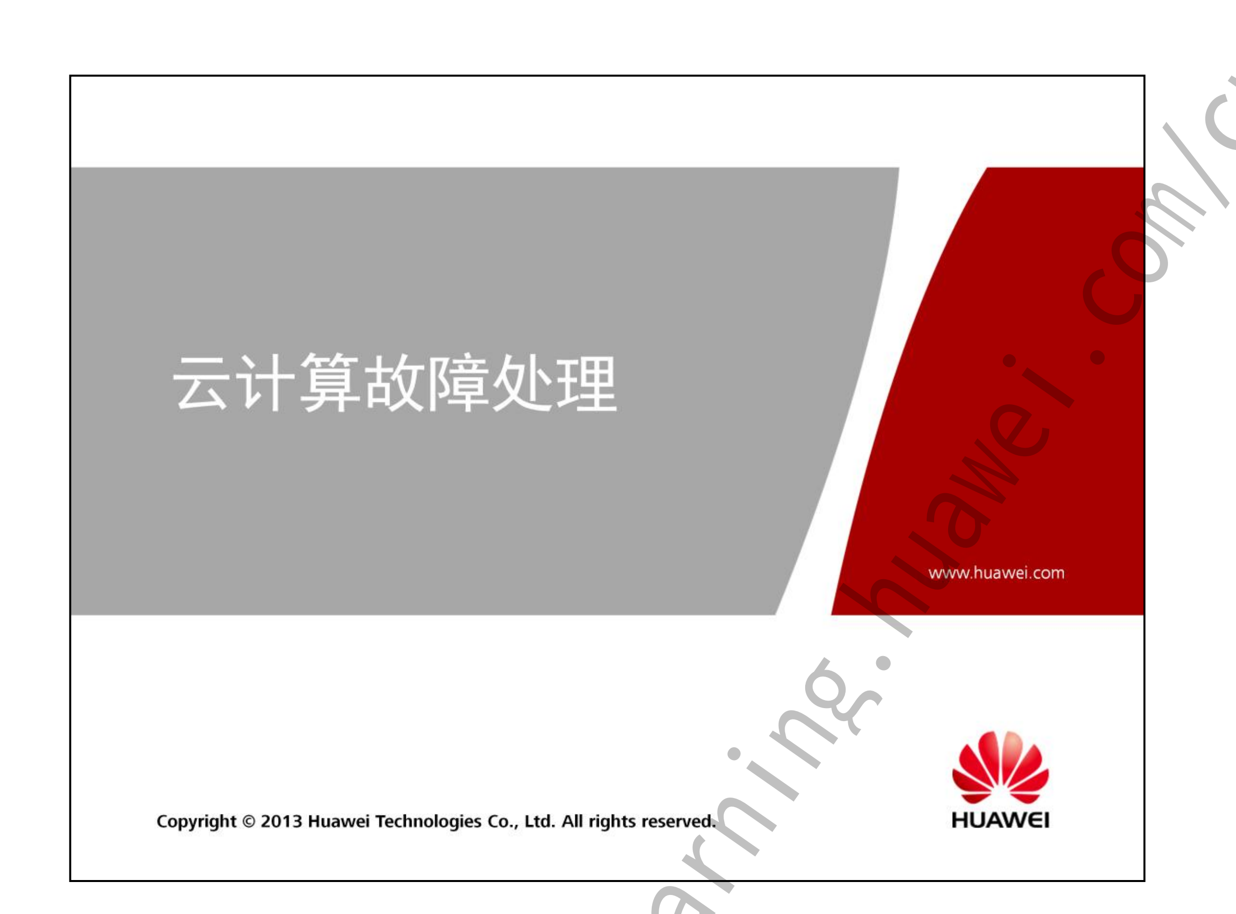
总结

- 云安全基本知识
- 终端及接入安全
- 网络安全
- 虚拟化软件安全
- 数据安全
- 运维安全
- 基础设施安全



Thank you

www.huawei.com


云计算故障处理
www.huawei.com
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



目录



故障处理流程

开始
收集并记录相关信息
是否能判断故障范围和类别？
否
是
确定故障范围和类别
定位故障原因
进行故障排除
故障是否被排除？
否
联系华为技术支持
是
记录故障处理过程
结束

- 故障处理流程：
  - 故障信息收集
  - 故障判断
  - 故障定位
  - 故障排除

 Page 3 

- 故障信息收集
  - 故障信息是故障处理的重要依据，系统维护人员应尽可能多的收集故障信息。
- 故障判断
  - 排除故障之前，系统维护人员根据收集的故障详细信息，对故障范围和类型进行判断。
- 故障定位
  - 故障定位是指从众多可能原因中找出故障原因的过程。通过一定的方法或手段分析、比较各种可能的故障成因，不断排除非可能因素，最终确定故障发生的具体原因。
- 故障排除
  - 故障排除是指根据不同的故障原因清除故障的过程。故障排除包括检修线路、修改配置数据、重启相关进程、重启服务器等。
  - 说明：当系统维护人员无法自行排除故障时，请联系华为技术支持。
- 确认故障是否被排除
  - 通过查询设备状态、查看设备指示灯和告警等方法确认系统已正常运行，并进行相关业务调测以确保业务正常。

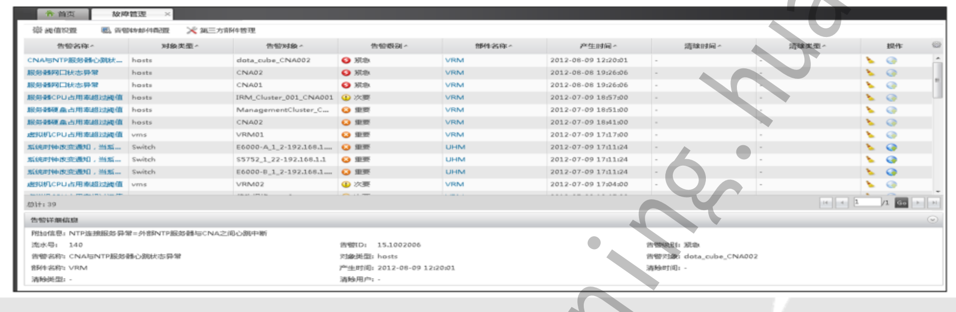
故障信息收集与判断

- 故障信息是故障处理的重要依据，维护人员应尽可能多的收集故障信息，包括：
  - 故障现象描述
  - 故障发生的时间及频率
  - 故障发生的地点
  - 故障的范围、影响
  - 故障发生前设备运行状况
  - 故障发生前对设备进行的操作以及操作的结果
  - 故障发生时是否有设备指示灯异常
- 维护人员根据收集的故障详细信息，对故障范围和类型进行判断



故障定位

- 常用故障定位方法：
  - 查看告警信息
  - 查看监控信息是否正常
  - 查询操作日志，分析操作过程是否有误
  - 检查数据配置是否正确
  - 观察设备指示灯状态是否正常





- 故障定位：维护人员需要从众多可能原因中找出故障原因的过程。

故障排除

- 根据定位结果进行故障排除处理：
  - 告警：如果发现告警与故障的产生现象相匹配，通过告警流程进行处理
  - 监控：由于性能原因导致系统故障时，需要进行扩容
  - 操作错误：根据操作日志发现进行了错误的操作时，需要对该操作进行恢复
  - 数据配置错误：检查配置数据时，对错误的数据进行更正
  - 硬件状态错误：根据硬件指示灯类型进行故障处理，如无电源指示时需要上电或重启，无数据传输时可插拔或更换连线等





目录



案例一：网络广播风暴（1/2）

- 操作场景
  - 网络访问变慢，丢包严重，时延较大，网络通信受到严重影响（丢包>0.1%，时延>20ms）
  - 交换机网络接口收发速率偏高，广播报文流量非常大，超过正常收发单播报文数量
  - 服务器CPU占用率高，接近100%
  - 服务器网卡收到的流量高，达到端口速率的80%
  - 对交换机端口进行抓包分析，下发大量重复的ARP广播报文

 Page 9



注意： 为避免误操作导致严重网络风暴影响业务通信，需注意如下事项：

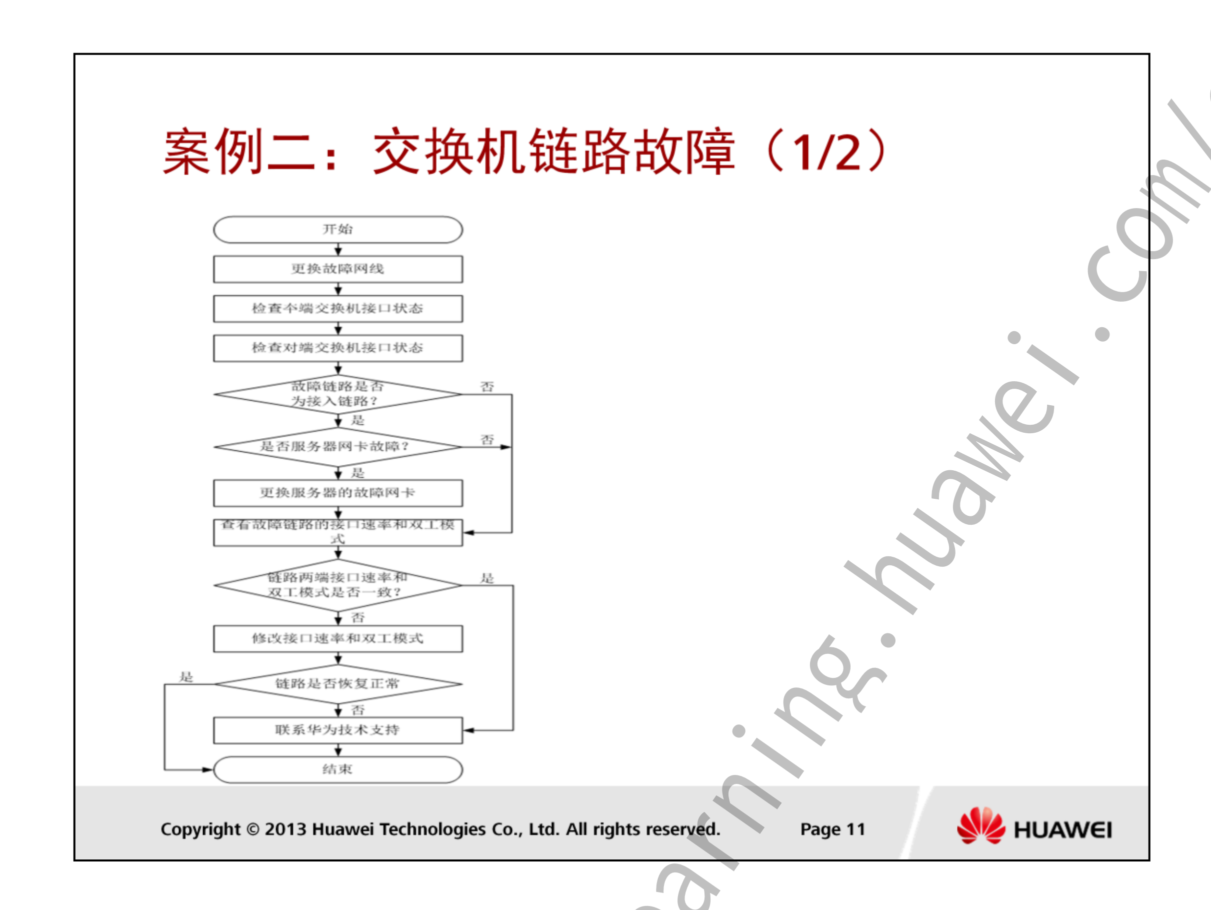
- 交换机上电之前，应确保交换机之间的连线只有一根。数据配置核对正常后，再连上所有交换机之间的连线。
- 数据规划时，应注意控制广播域的大小，不需要的VLAN和不需要通过的VLAN无需配置。
- 数据配置正常后，需要禁用不用的端口，避免误操作引发环路。
- 为减少广播风暴，可以针对易发生网络风暴的端口，配置风暴抑制功能，将广播报文的报文数抑制在5000pps以内，超出5000pps，该端口将被阻塞。
- 如果由于操作原因经常造成广播风暴，可以打开广播报文抑制功能，例如将广播报文比例抑制在30%以内。

案例一：网络广播风暴（2/2）

- 故障排除操作步骤
  - 排查配置变化
    - 1、检查操作日志，查看近期的配置修改情况；
    - 2、恢复现网数据配置；
    - 3、故障是否恢复?
      - 是，处理完毕。
      - 否，执行步骤 4
  - 排查物理环路
    - 4、检查交换机间物理连线；
    - 5、拆除环路连线；
    - 6、故障是否恢复。







- **对系统的影响**
  - 接入链路网络中断时，该链路所在CNA节点的虚拟机无法正常使用。
  - 干道链路网络中断时，该链路所在CNA节点的虚拟机无法进行HA或迁移。
  - Trunk链路网络中断时，所有虚拟机无法正常使用。
- **操作步骤**
- 更换故障链路的网线
  1. 巡检并找到故障链路。 当链路故障时，所连交换机接口的指示灯状态为熄灭。
  2. 更换网线。
  3. 链路是否恢复正常?

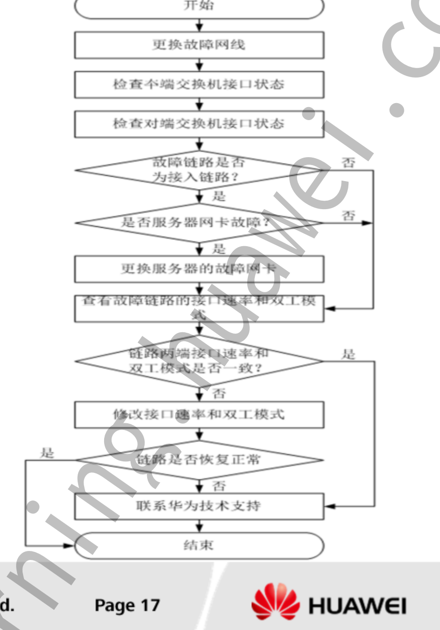
     是，处理完毕。

     否，步骤 4。
- 使用串口方式登录交换机

4. 使用终端仿真程序，建立PC机与交换机的串口通讯连接。 关键参数如下:
   - 交换机的端口位置：设备前面板右侧 “CONSOLE”口

案例二：交换机链路故障（2/2）

- 操作步骤
  - 更换故障链路的网线
  - 使用串口登录交换机
  - 检查本端交换机接口的状态
  - 检查故障链路是否为接入链路
  - 检查是否服务器网卡故障
  - 查看故障链路的接口速率和双工模式
  - 检查链路两端接口速率是否一致
  - 检查双工模式是否一致



 Page 17 HUAWEI

- 说明： 参数 “full”表示全双工， “half”表示半双工。

32. 链路是否恢复正常?

    是，处理完毕。

    否，请联系华为技术支持。

案例三：CNA网络无法建立连接（1/2）

- 操作场景
  - CNA节点上的虚拟机出现丢包现象，甚至出现网络不通的情况
  - “运维管理系统”监控中显示，该CNA节点状态为“未知”
  - “运维管理系统”告警中出现“ALM-15.1003002 存储链路中断”告警，稍后又被自动清除



案例三：CNA网络无法建立连接（2/2）

- 操作步骤
  - 查看日志文件：vi /var/log/messages
  - 查看连接跟踪数：最大连接跟踪数是否大于当前连接跟踪数90%
  - 修改最大连接跟踪数
  - 配置“TIME_WAIT”和“ESTABLISHED”的老化时间
  - 检查故障恢复情况

 Page 19



操作步骤

- 查看日志

1. 使用“PuTTY”，登录故障CNA节点操作系统。 以“root”用户，通过“管理平面IP地址”登录故障CNA节点。
2. 执行以下命令，查看日志文件。 **vi /var/log/messages**
3. 屏幕回显中是否出现大量的如下信息。 nf_conntrack: table full, dropping packet

   是，退出日志文件查看模式，并执行步骤 4。

   否，退出日志文件查看模式，并执行步骤 18。
4. 说明： 按“Esc”，并输入**:q**，可退出日志文件查看模式。
   - 查看连接跟踪数
5. 执行以下命令，查看最大连接跟踪数。 **cat /proc/sys/net/netfilter/nf_conntrack_max**
6. 执行以下命令，查看当前连接跟踪数。 **cat /proc/sys/net/netfilter/nf_conntrack_count**

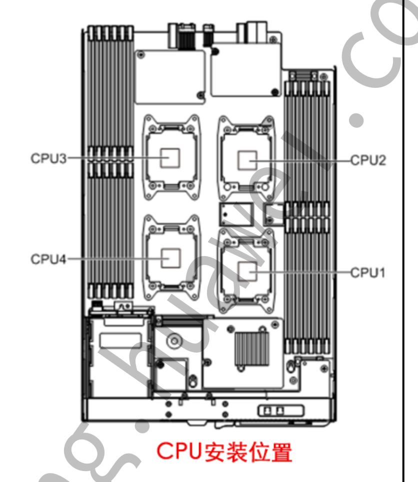


目录



案例一：服务器的CPU故障（E6000）

- 安装多个CPU 时，CPU 的型号必须相同
- 更换CPU过程如下
  - 佩戴好防静电腕带
  - 拆卸待更换CPU 所在的刀片
  - 打开刀片的外壳
  - 拆卸待更换的CPU
  - 安装新的CPU
  - 将已安装好CPU的刀片外壳装回
  - 将已安装好CPU 的刀片插回机箱





- 安装完成后，将刀片上电，进入BIOS 设置界面，查看CPU 信息是否正确

 Page 25 HUAWEI

- 安装、更换CPU 时，请注意以下事项：
  - 安装多个CPU 时，CPU 的型号必须相同
  - 当CPU 不满配时，请按照以下要求操作：
    - 只安装2 个CPU 时，必须安装在CPU1、CPU2 插座
    - 不能卸下未安装CPU 的插座上的保护盖
    - 未安装CPU 的插座上必须安装CPU 挡风板

- 步骤1 拆卸待更换的CPU：

1. 按照对角线的顺序逆时针旋转固定散热片的4 个螺钉，向上缓缓用力将散热片拔出；

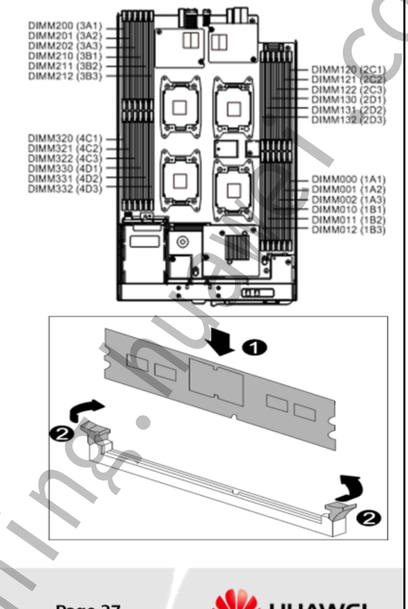
2. 首先沿 “OPEN 1st” 方向移动对应的CPU 锁定杆以将其释放，直到将锁定杆旋转到完全打开的位置；

3. 然后沿 “CLOSE 1st”方向移动对应的CPU 锁定杆以将其释放，直到将锁定杆旋转到完全打开的位置；

4. 打开CPU 底座的翻盖，将CPU 向上拔离插座。

案例二：服务器的DIMM故障（E6000）

- 更换DIMM过程如下
  - 佩戴好防静电腕带
  - 拆卸待更换DIMM所在的刀片
  - 打开刀片的外壳
  - 拆卸待更换的DIMM
  - 安装新的DIMM
  - 将已安装好DIMM的刀片外壳装回
  - 将已安装好DIMM的刀片插回机箱
- 安装完成后，将刀片上电，查看显示的内存容量和实际内存容量是否符合





 Page 27 HUAWEI

- 步骤 安装新的DIMM

1. 将备用的DIMM 从防静电包装袋中取出；

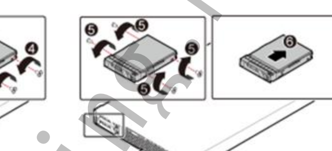
2. 确保内存插槽接口的两个固定夹都处于完全打开位置，调整DIMM 以使DIMM 上的缺口与插槽上缺口对齐；

3. 沿着插槽导轨将DIMM 竖直插入接口中；

4. 确保固定夹已锁住DIMM 且咬合紧密。

案例三：服务器的硬盘故障（E6000）

- 更换硬盘时务必保证同一RAID 组的硬盘同规格同型号
- 更换硬盘操作过程如下
  - 佩戴好防静电腕带
  - 根据RAID 配置信息，判断待更换硬盘是否在RAID 组内。
  - 拆卸待更换的硬盘
  - 安装新的硬盘
- 安装完成后，将刀片上电，通过观察硬盘指示灯的状态检测硬盘是否能够正常工作





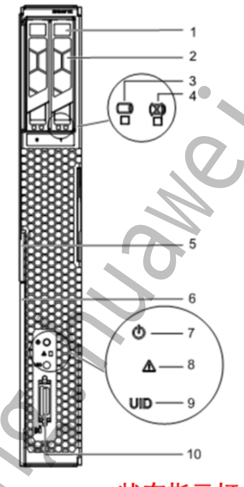
Page 28

HUAWEI

案例四：服务器指示灯告警（E6000）

- 面板上的状态指示灯出现（红色）闪烁
- 根据状态指示灯的闪烁频率定义告警级别，闪烁频率越高，表示告警越严重
- 通过iMana 的Web 界面查询告警的状态及日志
  - 客户端通过MM 模块连接到iMana 的管理网口
  - 登录iMana 的Web 界面
  - 进入“事件与日志 > 系统事件”界面查询告警的状态

  及日志
  - 查看告警帮助做相应的故障处理





HUAWEI

根据状态指示灯的闪烁频率定义告警级别，闪烁频率越高，表示告警越严重。

- 轻微告警：状态指示灯以0.5Hz 的频率闪烁（即2 秒闪烁1 次）。
- 严重告警：状态指示灯以1Hz 的频率闪烁（即1 秒闪烁1 次）。
- 紧急告警：状态指示灯以4Hz 的频率闪烁（即1 秒闪烁4 次）。



目录



案例一：1路级联链路故障

- 现象描述
  - IP SAN有大量不同磁盘单链路标记
  - 设备视图来看级联端口处于已连接状态，或亮红灯
  - IP SAN业务正常
- 可能原因
  - 光纤线折断或被拔出
  - 光纤线弯折或接触不良
  - 光模块老化或故障
  - 业务独立构件
- 处理步骤
  - 当光纤线故障时更换光纤线，当模块故障时更换光模块



案例二：RAID组中1块硬盘故障(1/2)

- 通过ISM查看IP SAN告警时，出现如下告警：
  - 硬盘SMART信息非法告警
  - 同一块硬盘有频繁的硬盘被拔出及硬盘插入的告警
  - 有较多硬盘被CTS旁路的告警
  - 硬盘失效或被拔出的告警
  - RAID组降级或热备盘失效的告警



案例二：RAID组中1块硬盘故障（2/2）

- 处理步骤
  - 在RAID组重构完成或磁盘预拷贝完成后更换故障硬盘
  - 登录CLI命令行，查看IP SAN的IO时延
  - 若查看到IP SAN的IO时延明显上升，尽快将故障盘拔出并更换

 Page 33 

- 处理步骤

1. 在RAID组重构完成或磁盘预拷贝完成后更换故障硬盘。
2. 如果出现现象描述中第2种和第3种情况，请尽快更换异常的硬盘并请联系华为技术支持。
3. 登录CLI命令行，查看IP SAN的IO时延。
    1. 当IP SAN类型为S5600时，执行如下命令后，执行步骤 5。
    2. **chgstatswitch -o -p**
    3. **statperf -p**
    4. 出现如下类型回显：CtrlID PortID RIO WIO RIOT(MB/s) WIOT(MB/s) CBW(MB/s) MBW(MB/s) CIOPS(IO/s) MIOPS(IO/s) MDelay(ms) ADelay(ms) A 00+01 0 0 0.000000 0.000000 0.000000 0.000000 0 0 0 0 B 02_03 0 0 0.000000 0.000000 0.000000 0.000000 0 0 0 0
    5. 当IP SAN类型为S3900时，执行步骤 4。

案例三：电源故障

- 当控制框单电源故障时
  - 查看ISM告警信息时，出现电源或风扇故障告警
  - 查看IP SAN控制框，电源指示灯点亮红灯
  - 在ISM上查看任意一个LUN的详细信息时，LUN的写属性均为透写
  - IP SAN提供的性能明显下降，导致该IP SAN所承载的用户虚拟机变慢，或者导致虚拟机不能登录
- 当级联框单电源故障时
  - 查看ISM告警信息，出现电源或风扇不正常的告警
  - 查看IP SAN级联框，电源指示灯点亮红灯

 Page 35





目录





TC损坏无法恢复

- **现象描述**

  TC无法启动或者配置。

- **可能原因**

  升级失败、配置错误、TC存在缺陷。

- **处理思路**

  恢复TC至出厂状态。

- **处理步骤**

Windows XPE TC处理步骤：	Linux TC处理步骤：
1、按TC开机按钮 2、开机过程中按“Ctrl” 3、出现菜单后，按“Ctrl+U” 4、选择“Restore Configuration”	1、按TC开机按钮 2、开机过程中按“F2” 3、出现菜单后，按“Exit”，弹出对话框 4、选择“Load Setup Defaults”



- 对TC进行升级或配置等操作，导致TC损坏，无法启动或无法进行配置。
- 如果上述方法无法排除故障，请更换TC，联系华为技术服务工程师。

TC无法升级

- **现象描述**

  使用TCM管理系统升级TC版本，TC无法进行升级。

- **可能原因**

  TC版本不匹配、TC设置归属TCM的IP地址错误、数据服务器系统中设定的TCM的IP地址错误。

- **处理思路**

  检查TC版本、检查IP地址。

- **处理步骤**

1、检查TC版本，确认版本匹配，其中包括安全版、自由版。
2、检查并设置正确TC上的TCM的IP地址，确保双方的IP地址能够连通，且中间无防火墙。
3、检查数据服务器中设定的管理服务器（TCM）的IP地址。



- TC升级文件必须匹配。TC的linux版本分自由和安全两种，如果升级前的TC为安全TC，则升级目标版本也应为安全TC；反之，亦然。否则会升级失败。
- 上传升级文件过程中如果数据服务器系统中设定的TCM的IP地址不正确，会导致数据服务器在TCM管理页面中处于离线状态，从而导致上传升级文件到数据服务器失败。
- 升级前需要到TC中设置CDMS config，如果TC中已指定归属TC管理器的IP地址，则需要确保IP地址正确，否则无法被TCM管理导致无法升级。

TCM常见问题与解决方法（一）

- **现象描述**

  无法添加数据服务器，提示IP或者端口错误

- **解决方法**
  - 确认数据服务器是否已经成功安装；
  - 确认数据服务器主机是否开启了防火墙，数据服务器默认工作端口9999、10021是否已经开放，可用命令“telnet 数据服务器IP 9999”进行诊断。

- **现象描述**

  CDMS安装完毕后UnitedWeb服务启动，却无法访问

- **解决方法**

  检查CDMS工作端口（默认443）是否被防火墙屏蔽。

 Page 39 

- 通过TCM可以实现客户机管理自动化，涵盖客户机配置、系统部署、软件分发、远程维护、性能监控、报警管理等多项功能；通过本系统，能够高效运维管控，彻底解决IT管理者面临的客户机部署、维护、配置等问题，同时通过集中管理，能够对企业IT 资源管理高度整合，大力提高企业IT 管理效率。

TCM常见问题与解决方法（二）

- **现象描述**

  TCM消息管理功能故障

- **解决方法**
  - 明确Xpe的TC支持消息回复，Linux TC不支持消息回复；
  - 从客户端回复的消息如果无法看见，请使用admin帐号登录再查看。

- **现象描述**

  TCM性能监控无法收到邮件通知

- **解决方法**
  - 性能监控的邮件通知功能，需要在TCM“公共管理” –>“其他管理” –>“全局参数设置”中的Mail设置中填写基本的信息；
  - 确保新建用户时候填写的用户邮箱是可用的，该邮箱地址可修改。





目录



FC、FM故障处理介绍

- 单点故障
  - VRM虚拟机故障
  - CNA节点OS故障
  - ESC 、IMGS虚拟机故障
- 双点故障
  - 主备VRM虚拟机同时故障
  - 主备 ESC虚拟机同时故障
  - 主备 GM 虚拟机同时故障



VRM虚拟机故障处理

- 现象描述：
  - VRM主备部署时，单个VRM虚拟机OS故障，且重启该虚拟机后仍无法登录
  - 出现“ALM-15.1002000 主备间节点心跳故障”告警
- 处理流程：

按照ALM-15.1002000告警处理方式处理
→ 查询故障VRM节点的信息关闭VRM虚拟机监控开关
→ 通过ISO挂载的方式重新安装故障VRM虚拟机
→ 配置主备关系（将重新加载OS的VRM节点配置为备节点）
→ 打开VRM虚拟机监控开关
→ 配置VRM节点ntp服务
→ 检查系统状态是否恢复成功

1.在按照该流程进行VRM虚拟机OS故障恢复之前，可以按照维护人员的经验可以先做尝试性的恢复，比如检查网络，在Portal上重启或者启动VRM虚拟机看是否能够恢复

2.上面流程中的关闭VRM虚拟机监控开关，主要防止在虚拟机重新加载过程中认为该VRM虚拟机异常而进行重启

3.如果故障节点使用的当前版本为补丁版本时，需要在OS加载完成后给节点安装补丁。

4.当VRM主备部署时，单个VRM虚拟机OS故障恢复，是无需重新导入备份数据的。

CNA节点OS故障处理

- 现象描述：
  - 主机不能正常登录或存在“ALM-10.1000027 心跳异常”的告警
- 可能原因：
  - 主机的操作系统故障
  - 主机的硬件故障
- 处理流程：

 Page 44 HUAWEI

1.在按照该流程进行CNA节点OS故障恢复之前，可以先按照ALM-10.1000027告警处理方式进行尝试性的恢复

2.在一体机场景下，如果遇到CNA节点OS或者影响层面的故障导致CNA节点异常，可以按照CAN节点部件更换流程进行操的方式恢复CNA节点作，该流程主要是针对非一体机场景，通过手动安装

3.上图流程中的“配置网络信息”：安装完操作系统后，需对主机网络信息进行配置，并确认配置的IP地址、主机名等信息和原主机保持一致。

4.上图流程中“恢复主机数据”，需要通过Putty登陆VRM节点执行恢复CNA节点数据的命令

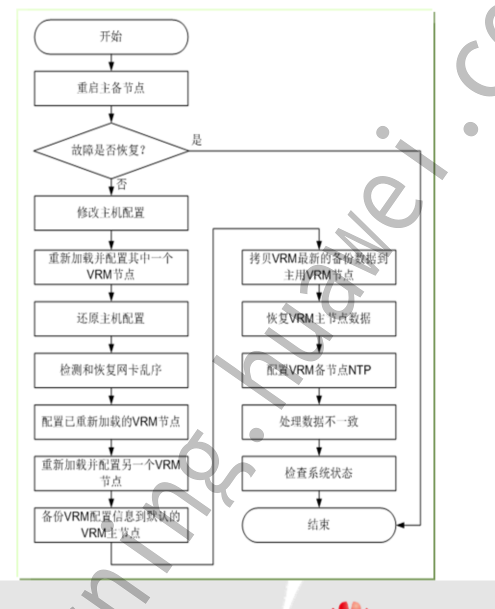
5.上图流程中的“恢复多路径数据”用于存储为非华为的存储设备场景，如果是华为设备则无需执行。

6.上图流程中的“备份VRM虚拟机的xml文件”，用于当主备VRM虚拟机都异常stop，可以通过在运行VRM虚拟机的主机上执行命令拉起，该命令依赖于该xml文件。

7. 如果故障节点使用的当前版本为补丁版本时，需要在OS加载完成后给节点安装补丁。

主备VRM虚拟机同时故障

- 故障场景：主备VRM虚拟机同时故障
- 对系统影响：
  - 无法新增业务，如创建虚拟机。
  - 无法对外提供监控告警、配置等运维服务
- 操作场景：
  - 在主备VRM同时故障时，要通过备份到第三方备份服务器的VRM管理数据进行数据恢复，如果数据没有备份到第三方备份服务器，该故障无法恢复。
  - 在恢复过程中需要使用“vncviewer.exe”工具





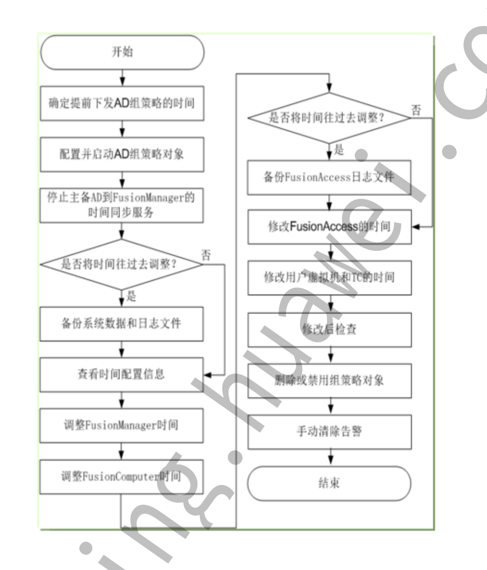


目录



系统时间故障

- 故障场景：系统时间故障
- 对系统影响：
  - 当FusionAccess系统部件的时间比FusionCompute系统时间快5分钟以上时，将导致业务发放不成功
- 操作场景：
  - 时间调整过程中，需中断所有业务，但不影响用户正在使用的虚拟机；若将时间调前，将影响业务受理
  - 修改后的系统时间，不能早于加载License的时间



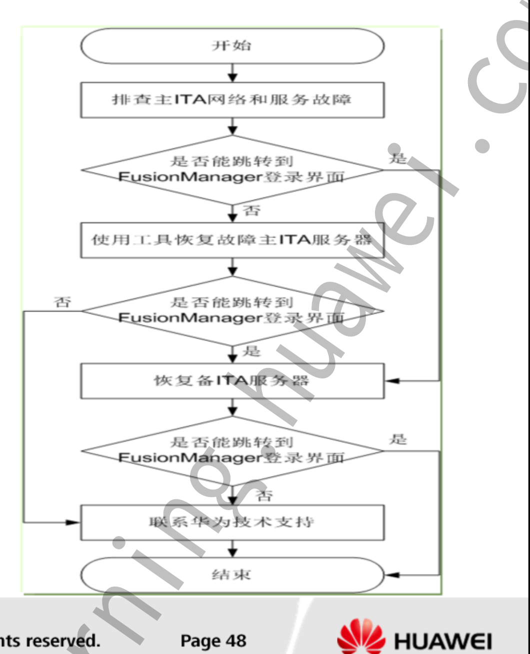
 Page 47



- 时间调前的影响
  - 如果将时间调整到当前时间之前的时间点，则需要中止该时间点到当前时间这一段时间的业务受理（如订单和用户审批）。如要将时间从00:00调整为23:00，则需要提前1小时停止业务受理。
  - 如果是将时间到当前时间之前的时间点，可能会覆盖掉系统历史的备份文件和日志文件。
- 可能造成故障的场景
  - 维护工程师在以下场景时，需要参考本故障处理进行全局时间调整，使系统时间恢复正常。
  - 系统未部署精确外部时钟源，长时间运行后系统整体时间出现了累积偏差。
  - 人为误操作调整了GM系统时间。
  - 人为误操作导致GE、VDI的某个节点的系统时间出现了累积偏差。
  - 系统时间同步失败导致GE、VDI的某个节点的系统时间出现了累积偏差。

主备ITA服务器同时故障

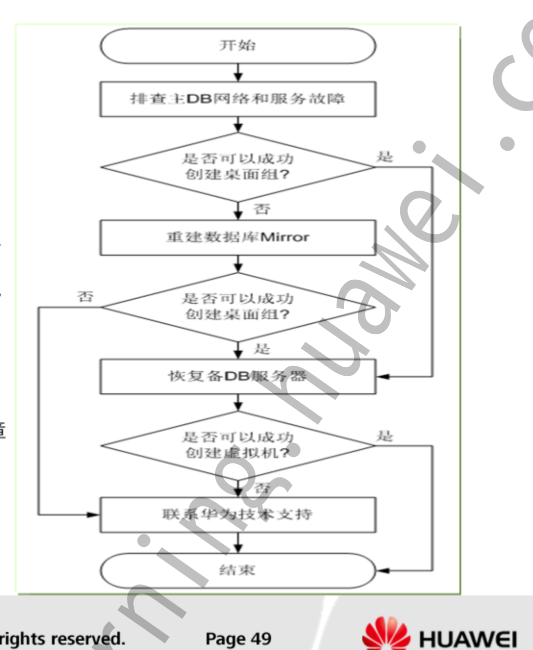
- 故障场景：主备ITA服务器同时故障
- 对系统影响：
  - ITA服务不可用，管理员无法创建虚拟机，无法对虚拟机进行管理，如查看、启动、重启、分配等
- 操作场景：
  - 在处理该故障前，需要处理ITA服务器所依赖的AD、DHCP、DNS、DB、DDC服务器的故障，确保其依赖的组件正常，具体操作请参见各组件对应的告警处理或者故障处理



HUAWEI

主备DB服务器同时故障

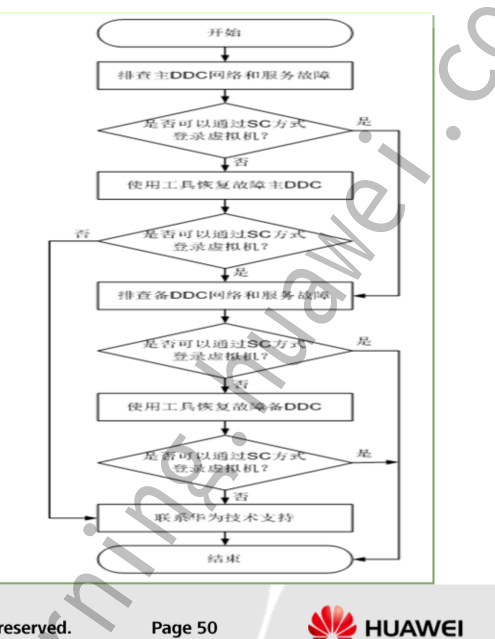
- 故障场景：主备DB服务器同时故障
- 对系统影响：
  - SQL Server服务不可用，管理员无法创建虚拟机，无法对虚拟机进行管理，如重启虚拟机、分配虚拟机等
- 操作场景：
  - 主备DB服务器所在虚拟机同时故障
  - 数据库的状态为In Recovery或者Suspended



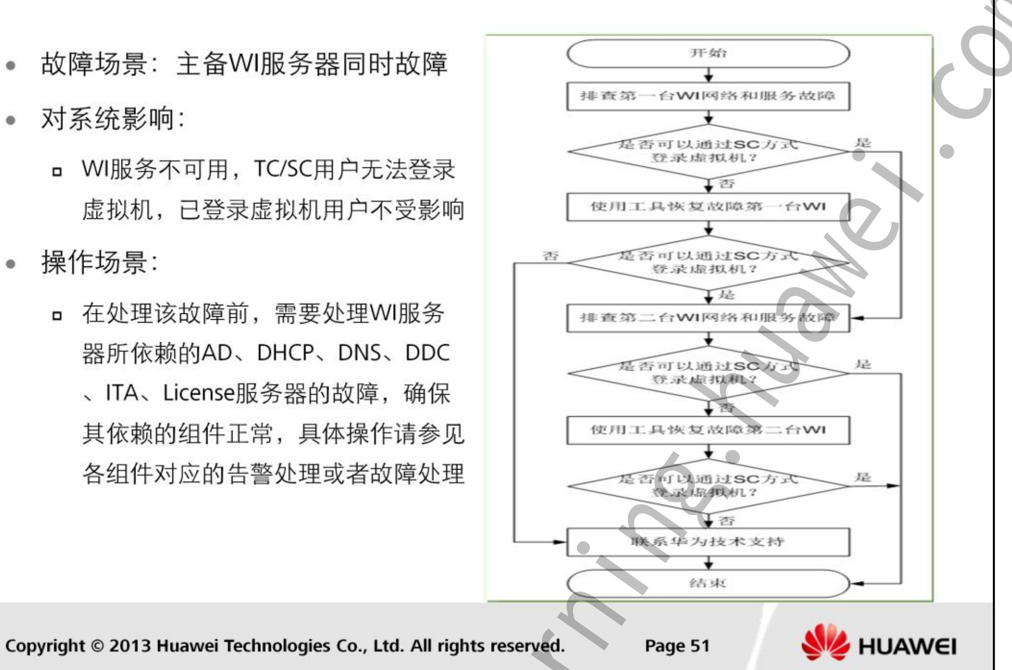
HUAWEI

主备DDC服务器同时故障

- 故障场景：主备DDC服务器同时故障
- 对系统影响：
  - DDC服务不可用，TC/SC用户无法登录虚拟机，已登录虚拟机用户不受影响
- 操作场景：
  - 在处理该故障前，需要处理DDC服务器所依赖的AD、DHCP、DNS、DB、License服务器的故障，确保其依赖的组件正常，具体操作请参见各组件对应的告警处理或者故障处理

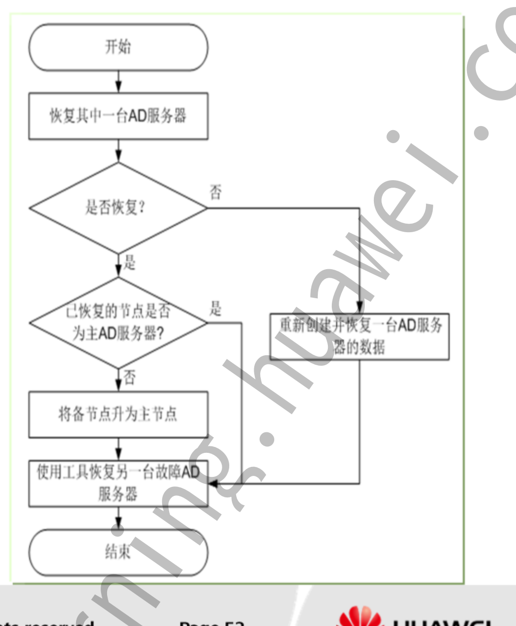


 Page 50 HUAWEI


主备WI服务器同时故障
故障场景：主备WI服务器同时故障
对系统影响：
WI服务不可用，TC/SC用户无法登录虚拟机，已登录虚拟机用户不受影响
操作场景：
在处理该故障前，需要处理WI服务器所依赖的AD、DHCP、DNS、DDC、ITA、License服务器的故障，确保其依赖的组件正常，具体操作请参见各组件对应的告警处理或者故障处理
开始
排查第一台WI网络和服务故障
是否可以通过SC方式登录虚拟机？
是
否
使用工具恢复故障第一台WI
是否可以通过SC方式登录虚拟机？
否
是
排查第二台WI网络和服务故障
是否可以通过SC方式登录虚拟机？
是
否
使用工具恢复故障第二台WI
是否可以通过SC方式登录虚拟机？
是
否
联系华为技术支持
结束
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 51
HUAWEI

主备AD服务器同时故障

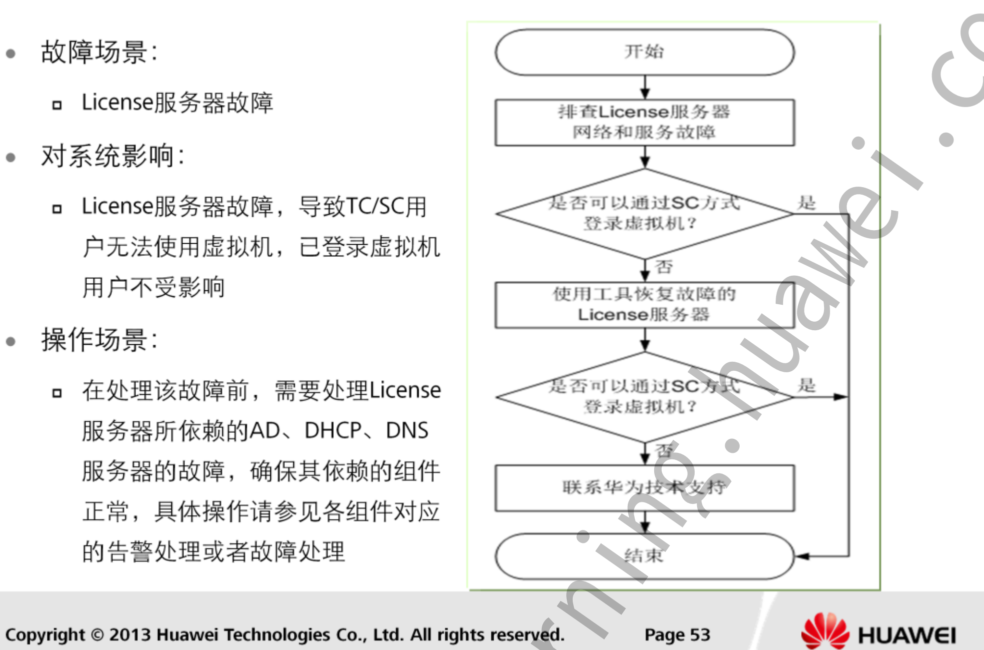
- 故障场景：主备AD服务器同时故障
- 对系统影响：
  - 在AD服务器恢复的过程中，系统管理员无法用域帐户登录基础架构服务器，虚拟机用户无法登录虚拟机
- 操作场景：
  - 在系统的主、备AD服务器同时故障的场景下，通过新建服务器并恢复配置文件及其数据库来排除故障



HUAWEI

License服务器故障

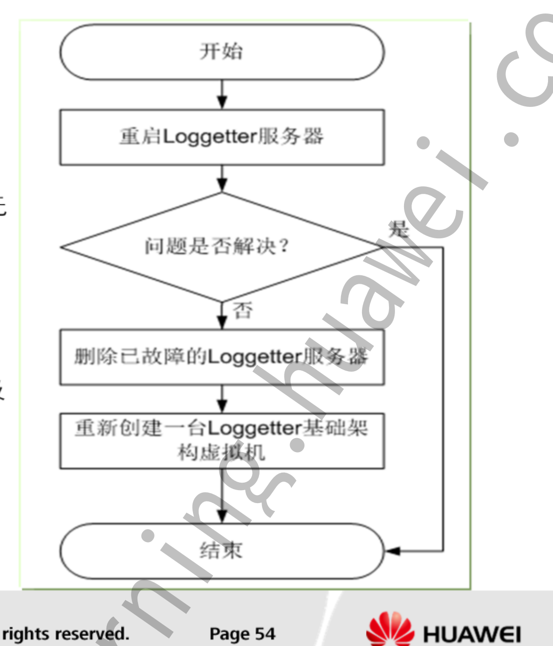
- 故障场景：
  - License服务器故障
- 对系统影响：
  - License服务器故障，导致TC/SC用户无法使用虚拟机，已登录虚拟机用户不受影响
- 操作场景：
  - 在处理该故障前，需要处理License服务器所依赖的AD、DHCP、DNS服务器的故障，确保其依赖的组件正常，具体操作请参见各组件对应的告警处理或者故障处理



 Page 53 HUAWEI

Loggetter服务器故障

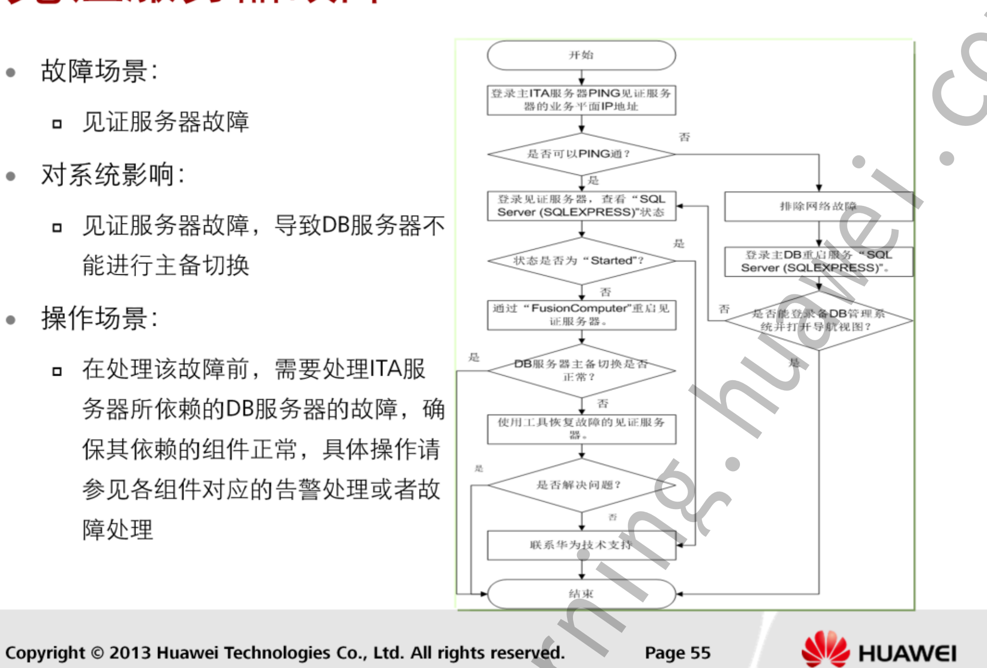
- 故障场景：
  - Loggetter服务器故障
- 对系统影响：
  - Loggetter服务器不可用，导致其无法收集系统日志文件、备份数据
- 操作场景：
  - 在Loggetter服务器故障的场景下，通过新建服务器并恢复配置文件及其数据库来排除故障



HUAWEI

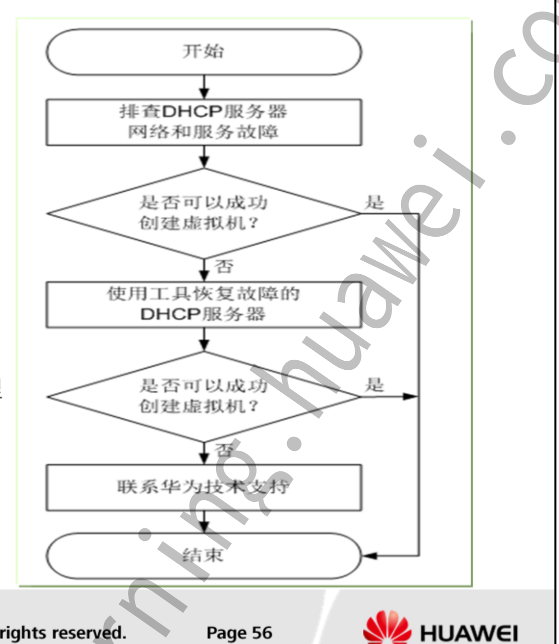
见证服务器故障

- 故障场景：
  - 见证服务器故障
- 对系统影响：
  - 见证服务器故障，导致DB服务器不能进行主备切换
- 操作场景：
  - 在处理该故障前，需要处理ITA服务器所依赖的DB服务器的故障，确保其依赖的组件正常，具体操作请参见各组件对应的告警处理或者故障处理



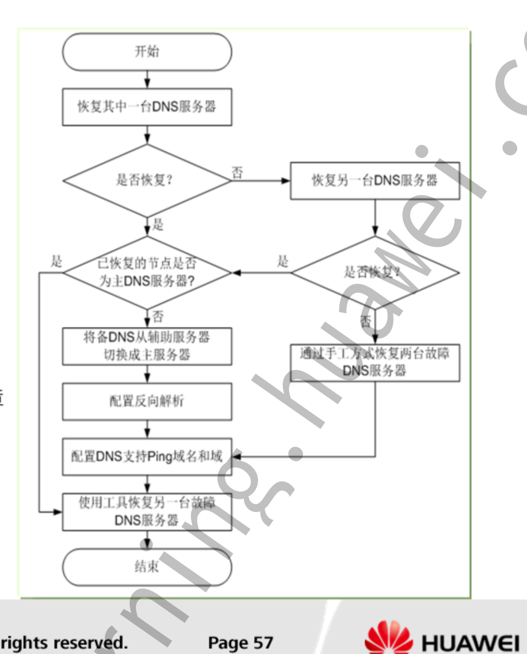
DHCP服务器故障

- 故障场景：
  - DHCP服务器故障
- 对系统影响：
  - DHCP服务器不可用，导致用户虚拟机无法获取IP地址，无法使用
- 操作场景：
  - 维护工程师在DHCP服务器所在虚拟机故障时，需要参考本故障处理操作，使业务快速恢复正常



主备DNS服务器同时故障

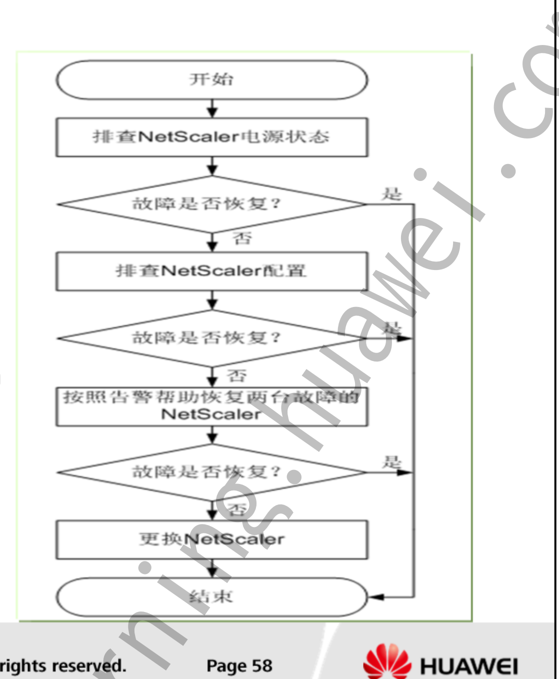
- 故障场景：
  - 主备DNS服务器同时故障
- 对系统影响：
  - 主备DNS服务器同时故障，导致用户无法通过域帐号登录虚拟机
- 操作场景：
  - 维护工程师在主备DNS服务器所在虚拟机同时故障时，可参考本故障处理操作，使业务快速恢复正常。



 Page 57 HUAWEI

主备NetScaler故障

- 故障场景：
  - 主备NetScaler故障
- 系统影响：
  - 所有ICA链接的虚拟机无法使用，RDP链接的虚拟机不受影响
- 操作场景：
  - 当主备NetScaler同时故障时，维护工程师需要参考本故障处理操作，使业务快速恢复正常





目录





目录



重大事故界定

- 重大事故
  - 指发生突然、影响面广、涉及范围大、并可对网络的安全运行与服务质量造成严重后果的设备或网络事故
  - 包括双节点故障、机柜异常掉电等
- 应急处理
  - 在系统或设备发生紧急事故的情况下，为迅速排除故障、恢复系统或设备的正常运行，从而尽量挽回或减少事故损失而对设备进行的一种故障处理行为

 Page 61




故障分类
故障分类
用户虚拟机故障
虚拟机蓝屏
大量虚拟机停止响应或磁盘丢失
系统时间故障
一体机时间管理应急指导
管理节点故障
主备VRM虚拟机同时故障
VRM节点DRBD故障
VDI服务器故障
主备ITA服务器同时故障
主备DB服务器同时故障
主备DDC虚拟机同时故障
主备WI虚拟机同时故障
主备AD服务器同时故障
License服务器故障
Loggetter服务器故障
见证服务器故障
DHCP服务器故障
主备DNS服务器同时故障
网络链路故障
交换机链路故障
CNA网络无法建立连接
硬件设备故障
主备NetScaler故障
设备供电故障
系统全局掉电故障
一体机基本机柜掉电故障
一体机扩展机柜掉电故障
系统交流供电中断故障（仅由UPS供电）
Copyright © 2013 Huawei Technologies Co., Ltd. All rights reserved.
Page 62
HUAWEI



目录



应急处理流程和原则（1）

- 应急处理流程：如右图所示
- 快速恢复原则：应综合考虑相应操作恢复业务成功的可能性和时间代价。参考的操作排序如下：
  - 耗时比较短，成功可能性比较大的操作
  - 耗时比较短，成功可能性比较小的操作
  - 耗时比较长，成功可能性比较大的操作

Page 64
HUAWEI

- **重大事故处理原则**

  由于重大事故很容易导致大面积的用户虚拟机故障、设备瘫痪等严重后果，具有很大的危害性。为提高重大事故的处理效率、并最大限度降低此类事故的损失，在维护本设备之前，应充分考虑并遵循以下应急处理的基本原则。

  - 应急处理以快速恢复设备的正常运行与业务的提供为核心，因此，提高重大事故处理效率的关键是：客户应参考应急处理手册及时制定各种重大事故的处理预案，并定期组织相关管理人员与维护人员进行学习、演练。
  - 以客户业务尽快恢复，对客户影响最低为原则。在此前提下，进行问题定位恢复和数据收集。
  - 维护人员在上岗前必须接受必要的应急处理培训，学习判断重大事故的基本方法、掌握处理重大事故的基本技能。
  - 在重大事故的处理过程中，维护人员应及时联系华为公司客户服务中心或华为公司驻当地办事处，以便能够快速获取华为公司的技术支持。
  - 当维护人员完成重大事故的处理以后，应该及时采集与本次事故有关的设备故障告警信息，并将相关的事故处理报告、设备告警文件、日志文件等发送给华为公司相应部门进行分析与定位，以便华为公司能够更好地为客户提供售后服务。

应急处理流程和原则（2）

- 重大事故处理原则
  - 以快速恢复设备的正常运行与业务的提供为核心
  - 以客户业务尽快恢复，对客户影响最低为原则
  - 维护人员在上岗前必须接受必要的应急处理培训
  - 在重大事故的处理过程中，维护人员应及时联系华为公司客户服务中心或华为公司驻当地办事处
  - 当维护人员完成重大事故的处理以后，应及时采集与本次事故有关的设备故障告警信息，并将相关的事故处理报告、设备告警文件、日志文件等发送给华为公司相应进行分析与定位

 Page 66



- 由于重大事故很容易导致大面积的用户虚拟机故障、设备瘫痪等严重后果，具有很大的危害性。为提高重大事故的处理效率、并最大限度降低此类事故的损失，在维护本设备之前，应充分考虑并遵循以下应急处理的基本原则。



目录



应急日常准备

类别	要求
设备级备份	• 主备用设备要求：定期进行数据一致性检查，以及运行状态检查，确保应急时能够接管业务。 • 负荷分担设备要求：定期进行负荷评估，评估业务单平面运行性能评估，确保单点故障业务可以全部由另一个设备接管。
（可选）容灾	容灾局及相关切换准备。
备件	关键设备需要常备备件。
日常告警清理	日常告警需要及时处理，确保没有未确认的活动告警，避免出现问题时，信息混乱，影响事故处理中的判断决策。
基本信息	维护人员需要准备以下基本信息： • 组网信息 • 设备基础信息 • 软件列表 • 网络设备IP地址信息 • 业务信息 • 备件信息 • 远程维护信息 • 相关接口人
人员技能要求	维护人员需要熟悉以下知识： • Linux基本操作命令 • 维护网络的组网与数据规划 • 基本TCP/IP原理、路由原理和交换原理 • 交换机、防火墙等网络设备的基本配置及操作 • 服务器、存储等硬件设备的基本原理 • GalaXEngine、VDesktop6000等软件部件的组成、工作原理和业务流程

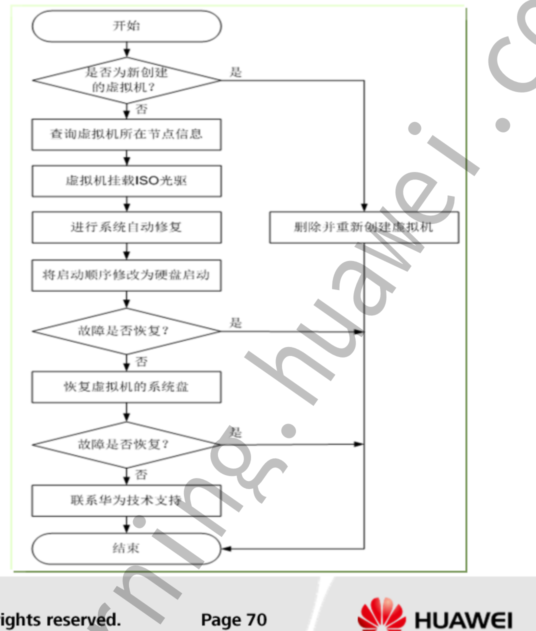


目录



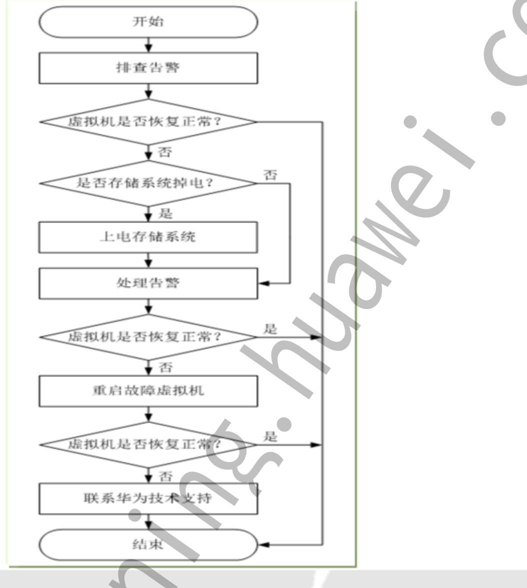
虚拟机蓝屏

- 故障场景：
  - 虚拟机蓝屏
- 对系统影响：
  - 该操作对系统正常运行无影响
- 操作场景：
  - 在用户虚拟机蓝屏或者黑屏时，需要参考本故障处理为虚拟机挂载ISO光驱，并对虚拟机操作系统进行修复操作，使虚拟机快速恢复正常



大量虚拟机停止响应或磁盘丢失

- 故障场景:
  - 大量虚拟机停止响应或磁盘丢失
- 对系统影响:
  - 该操作对系统正常运行无影响
- 操作场景:
  - 大量虚拟机系统停止响应，重启虚拟机失败。
  - 大量虚拟机的磁盘丢失或不可访问





虚拟机操作失败案例

案例一：模板导入虚拟机失败

故障描述： 模板导入虚拟机失败

可能原因： 模板文件共享目录权限设置错误

处理步骤：

1.登录FusionCompute，进入任务中心查看任务详细信息

2.在任务中心的对应任务详细信息中，找到失败原因：主机无法连接共享目录，请检查共享目录权限。

3.查看本机上的文件夹的共享配置是否正确，将模板文件所在目录共享给本机用户。再次执行模板导入虚拟机。



虚拟机操作失败案例

案例二：模板部署虚拟机失败

故障描述：模板导入虚拟机失败

可能原因：模板部署虚拟机最后阶段虚拟机在主机上启动失败；创建磁盘失败；系统拷贝磁盘失败；CPU资源不足。

处理步骤：

1.登录FusionCompute，进入任务中心查看任务详细信息

2.如果找到失败原因为“虚拟机在主机上启动失败”，则可能是创建虚拟机成功但是启动虚拟机失败，检查主机的管理网络通信是否正常。

3. 如果失败原因为“供选择的主机均异常”，检查主机的电源状态是否正常，主机的管理网络通信是否正常。



虚拟机操作失败案例

案例二：模板部署虚拟机失败

处理步骤续:

4.如果失败原因为“创建磁盘失败”，检查存储设备状态是否正常，或者数据存储剩余容量是否充足。

5.如果失败原因为“CPU资源不足，请检查CPU核数、预留、上限。”，检查集群资源是否充足，或者虚拟机绑定的主机资源是否充足。



虚拟机操作失败案例

案例三：创建裸虚拟机启动失败

故障描述：采用绑定主机的方式创建裸虚拟机成功但启动失败

可能原因：内存资源不足

处理步骤：

1.登录FusionCompute，选择“虚拟数据中心管理 > 虚拟机和模板”。

2.在该虚拟机任务跟踪中的查看对应任务（启动虚拟机）详细信息，找到失败原因：内存 资源不足。

3.选择“虚拟数据中心管理 > 主机与集群”。查看该虚拟机绑定主机的概要信息。确认该主机的监控信息中内存“可用容量”是否小于创建虚拟机的内存。如果是则执行第4步。



虚拟机操作失败案例

案例三：创建裸虚拟机启动失败

4.返回“虚拟数据中心管理 > 虚拟机和模板”。在“概要”页面进行“解绑定”，重新选择一个内存资源充足的主机绑定再重新启动即可。







总结

- 故障处理流程
- 硬件设备常见故障分析
- 软件系统常见故障分析
- 实际案例



Thank you

www.huawei.com

华为职业认证通过者权益

通过**任一项**华为职业认证，您即可在华为在线学习网站(*http://learning.huawei.com/cn*) 享有如下特权：

- **1、华为E-learning 课程学习**
  - **内容**：**所有华为职业认证E-Learning课程**，扩展您在其他技术领域的技术知识
  - **方式**：请提交您的“华为账号”和注册账号的“email地址”到 *Learning@huawei.com 申请权限。*
- **2、华为培训教材下载**
  - **内容：华为职业认证培训教材+华为产品技术培训教材，**覆盖企业网络、存储、安全等诸多领域
  - **方式**：登录*华为在线学习网站*，进入“*华为培训->面授培训*”，在具体课程页面即可下载教材。
- **3、华为在线公开课(LVC)优先参与**
  - **内容**：企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师授课，开班人数有限
  - **方式**：开班计划及参与方式请详见LVC排期：
    http://support.huawei.com/learning/NavigationAction!createNavi#navi[id]=_16
- **4、学习工具 eNSP**
  - *eNSP (Enterprise Network Simulation Platform)*，是由华为提供的免费的、可扩展的、图形化网络仿真工具。主要对企业网路由器和交换机进行硬件模拟，完美呈现真实设备实景；同时也支持大型网络模拟，让大家在没有真实设备的情况下也能够进行实验测试。
- 另外，华为建立了知识分享平台 华为认证论坛。**您可以在线与华为技术专家交流技术，与其他考生分享考试经验，一起学习华为产品技术。** （ http://support.huawei.com/ecommunity/bbs/list_2247.html ）

